1/2023

DVD Deutsche Vereinigung für Datenschutz e.V.

Datenschutz Nachrichten

46. Jahrgang
ISSN 0137-7767
14,00 Euro



■ Ein Überblick über die Digitalstrategie der Europäischen Union ■ Datenschutz und Datenhandel – Friktionen in der europäischen Digitalpolitik ■ EHDS – der Europäische Gesundheitsdatenraum ■ Digitalisierung und Datenschutz: Schluss mit Ausreden! ■ Pressemitteilungen ■ Nachrichten ■ Rechtsprechung ■ Buchbesprechungen ■

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Inhalt

Termine



Dienstag/Mittwoch, 25./26.04.2023
Datenschutztage 2023
FFD (virtueller Kongress)

Freitag, 28.04.2023
Verleihung der BigBrotherAwards
Hechelei Bielefeld

Samstag, 29.04.2023
Vorstandssitzung der DVD
Bielefeld

Montag, 01.05.2023
Redaktionsschluss DANA 2/2023
„Europäische Entwicklungen – Teil 2“

Donnerstag/Freitag 04./05.05.2023
Fachtagung „Datenschutz im Gesundheitswesen“
Bitkom mit BvD, GDD u.a., Berlin

Dienstag/Mittwoch, 09./10.05.2023
BvD-Verbandstage
Berlin

Montag-Mittwoch, 05.-07.06.2023
re:publica
Festival für die digitale Gesellschaft
Berlin (re-publica.com/de)

Montag/Dienstag, 12./13.06.2023
DuD-Datenschutzkongress 2023
Berlin

Foto: Pixabay..com

DANA
Datenschutz Nachrichten
ISSN 0137-7767
46. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Reuterstraße 157, 53113 Bonn
Tel. 0228-222498
IBAN: DE94 3705 0198 0019 0021 87
Sparkasse KölnBonn
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Thilo Weichert und Achim Klabunde
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Reuterstraße 157, 53113 Bonn
dvd@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autorinnen und Autoren.

Layout und Satz
Frans Jozef Valenta, 53119 Bonn
valenta@datenschutzverein.de

Druck
Onlineprinters GmbH
Dr.-Mack-Straße 83
90762 Fürth
www.onlineprinters.de
Tel. +49 (0) 9161 6209800
Fax +49 (0) 9161 8989 2000

Bezugspreis
Einzelheft 14 Euro. Jahresabonnement 48 Euro (inkl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos. Nach einem Jahr kann das Abonnement jederzeit mit einer Frist von einem Monat gekündigt werden. Die Kündigung ist schriftlich an die DVD-Geschäftsstelle in Bonn zu richten.

Leserbriefe
Leserbriefe sind erwünscht. Deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen, Fotos
Pixabay, iStock, OpenAI – DALL-E,
Frans Jozef Valenta
Titel: iStock – NicoElNino

Editorial

Mit der Datenschutz-Grundverordnung hat die EU einen Anlauf genommen auch die sogenannten Tech-Giganten an die Grundrechte und Regeln des Rechtstaats zu binden. Auch wenn Datenschutzaktivisten schon am ersten Tag der DSGVO-Anwendung ihre Beschwerden insbesondere bezüglich der verschiedenen Dienste von Facebook (heute Meta) eingereicht haben, hat es doch bis vor wenigen Wochen gedauert, bis die irische Datenschutzbehörde sich zu einer Sanktionsentscheidung durchgerungen hat. Und es bedurfte des koordinierten Einsatzes der anderen nationalen Datenschutzbehörden der EU, um über den Europäischen Datenschutzausschuss (EDSA) eine solche Entscheidung zu erzwingen. Die nächste Runde wird vor den europäischen Gerichten stattfinden: Meta wird zunächst in Irland klagen, die irische Datenschutzbehörde will gleich auf europäischer Ebene gegen Teile des EDSA-Beschlusses vorgehen. Es bleibt also spannend (mehr im Nachrichtenteil).

Nichtsdestoweniger hat sich auf der EU-Ebene die Erkenntnis durchgesetzt, dass es mehr als der Möglichkeiten einzelner Mitgliedstaaten bedarf, um sich gegen die Mega-Unternehmen der GAFAM durchzusetzen. Das ist der Ursprungsgedanke der EU-Digitalstrategie, die unter anderem wettbewerbsrechtliche Regeln, Verbraucherschutz und Verpflichtungen gegen die Verbreitung von Falschinformationen und Hasspropaganda für den ganzen EU-Binnenmarkt festlegen und mit Durchsetzungsmöglichkeiten versehen will.

Außer der stärkeren Kontrolle der Großunternehmen strebt der EU-Gesetzgeber auch eine Stärkung von EU-Unternehmen mit datenbasierten Geschäftsmodellen an. Dazu sollen Mechanismen zum Teilen von Daten zwischen verschiedenen Organisationen unterstützt werden.

Bisher besteht das Paket aus fünf Verordnungen: Digital Services Act, Digital Markets Act, Data Governance Act, Data Act und der Verordnung über den Europäischen Gesundheitsdatenraum (EGDR). Die ersten drei Instrumente sind bereits verabschiedet, die anderen beiden sind in fortgeschrittenen Verhandlungen zwischen den EU-Institutionen. Ziel der Kommission wird es sicher sein das Paket vor den Wahlen zum Europaparlament im Frühjahr 2024 abzuschließen.

Wir bringen zunächst einen Überblick über die Gesamtinitiative. Wobei wir auch an zwei Vorschläge erinnern, die strenggenommen nicht dazu gehören, nämlich den Rechtsakt über künstliche Intelligenz, der gerade verhandelt wird, und die ePrivacy-Verordnung, die jetzt seit sechs Jahren festhängt.

Professor Eric Hilgendorf gibt eine Einschätzung der von der Kommission vorgeschlagenen Pakete. Einige der Kritikpunkte mögen im Rahmen des Gesetzgebungsprozesses berücksichtigt worden sein. Ute Bernhardt, Ingo Ruhmann und Thilo Weichert tragen eine detaillierte und fundierte Analyse des Vorschlags zum EGDR bei.

Der BfDI Ulrich Kelber hat bei netzpolitik.org eine umfassende Kritik zu den verbreiteten Falschaussagen zum Datenschutz veröffentlicht, die wir mit großer Zustimmung nachdrucken.

Zum Abschluss gibt es offene Briefe (die teilweise auch) von der DVD mitunterzeichnet wurden sowie unsere Presseerklärung zur Registerveröffentlichung (inklusive einem Update) und es folgen wie immer die aktuellen Nachrichten, Urteile und Buchbesprechungen.

Wir wünschen Ihnen und Euch eine angenehme und anregende Lektüre.

Autorinnen und Autoren dieser Ausgabe:

Ute Bernhardt
Netzwerk Datenschutzexpertise, Berlin
bernhardt@netzwerk-datenschutzexpertise.de

Prof. Eric Hilgendorf
Universität Würzburg, Forschungsstelle RoboRecht
sekretariat.hilgendorf@jura.uni-wuerzburg.de

Prof. Ulrich Kelber
Bundesbeauftragter für den Datenschutz und die Informationsfreiheit, Bonn
poststelle@bfdi.bund.de

Achim Klabunde
DVD-Vorstandsmitglied, Bonn
klabunde@datenschutzverein.de

Ingo Ruhmann
Netzwerk Datenschutzexpertise, Berlin
ruhmann@netzwerk-datenschutzexpertise.de

Dr. Thilo Weichert
DVD-Vorstandsmitglied,
Netzwerk Datenschutzexpertise, Kiel
weichert@datenschutzverein.de

Achim Klabunde

Ein Überblick über die Digitalstrategie der Europäischen Union

Die aktuelle Europäische Kommission hat sich die Neuordnung der Rahmenbedingungen für digitale Dienste und die Märkte als Flaggschiffprojekt an die Fahne geheftet. Besonders die Kommissionsmitglieder Margarete Vestager und Thierry Breton werden als die Treiber der Initiativen wahrgenommen.

Frau Vestager hat bereits in ihrer letzten Amtszeit als Wettbewerbskommissarin die Möglichkeiten und Grenzen des EU-Wettbewerbsrechts ausgetestet. Das allgemeine Gericht der EU hat erst im September eine Wettbewerbsstrafe von über 4 Milliarden Euro gegen Google für wettbewerbswidrige Maßnahmen für rechtmäßig gehalten. Zwar hat Google in diesem, wie auch in anderen Fällen, noch die Möglichkeit Revision beim Europäischen Gerichtshof einzulegen, aber die erstinstanzliche Bestätigung stärkt natürlich die Position der Kommission.

Thierry Breton wird als Vorstand europäischer IT-Unternehmen sicherlich umfangreiche Erfahrungen mit den Tricks der IT-Riesen von der US-Westküste gesammelt haben. Der Digital Markets Act der EU zielt darauf ab mehr Wettbewerb für neue Unternahmen zu ermöglichen und erheblich schneller gegen wettbewerbswidriges Verhalten vorgehen zu können.

Aber Wettbewerb ist nur eine der Stoßrichtungen der Digitalisierungsstrategie der Kommission. Auch die Verbraucher sollen besser gegen Hasspropaganda und Falschinformationen geschützt werden. Das Instrument dazu ist der Digital Services Act. Er erlaubt es sehr große Plattformen, wie soziale Medien und Suchmaschinen, als „Torwächter" zu benennen, die dann strengeren Verpflichtungen unterliegen gegen Missbrauch ihrer Dienste vorzugehen.

Außer den verbesserten Wettbewerbs- und Verbraucherschutzbedingungen bemüht sich die EU auch datenbasierte Geschäftsmodelle zu ermöglichen. Erster Baustein der Datenstrategie ist der bereits beschlossene Data Governance Act (DGA). Dieser legt Bedingungen und Verfahren fest, wie Daten von Dateninhabern weiteren Akteuren zur Verfügung gestellt werden können. Der Schutz der Grundrechte der Personen, deren Daten verarbeitet werden, soll unberührt bleiben. Da der Gesetzgeber nur den allgemeinen Grundsatz festlegen konnte, wird sich die Auflösung von Konflikten wohl erst in der praktischen Anwendung entwickeln. Ein neues Konzept des DGAs ist auch der Datenaltruismus zur Bereitstellung von Daten im Interesse des Gemeinwohls.

Basierend auf dem DGA sollen weitere Instrumente zur Konkretisierung der Bedingungen für die Datenwirtschaft beschlossen werden. Der Data Act beinhaltet weitere Details der Datennutzung, z.B. über den Zugriff auf Daten von Benutzergeräten oder für den Zugang für Aufgaben der öffentlichen Verwaltung. Konkretisiert werden sollen Regeln für den Datengebrauch durch sektorspezifische Regeln. Am weitesten fortgeschritten ist der Europäische Gesundheitsdatenraum (EHDS), über den bereits Gespräche zwischen Rat und Europaparlament stattfinden. Der nächste Sektor könnte sich mit Mobilitätsdaten befassen und zum Beispiel den lange bestehenden Konflikt zwischen Fahrzeugherstellern und anderen am Verkehrsgeschehen beteiligten Parteien über die immer umfangreichere Datensammlung im Fahrzeugbetrieb angehen. Insgesamt hat die Kommission acht europäische Datenräume skizziert.

Außer an die aktuellen Gesetzesvorhaben erinnern wir in der nachfolgenden Übersicht auch an bereits länger laufende Verfahren. Der AI Act wurde vorgeschlagen, als der letzte AI-Hype losging und nähert sich ebenfalls möglichen konkreten Verhandlungen.

Bereits seit 2017 hängt die ePrivacy-Verordnung im Gesetzgebungsverfahren fest. Während das Europaparlament sich mehrheitlich für starke Bürgerrechte ausspricht, blockieren im Rat zum einen die Verfechter der wirtschaftlichen Nutzung von Kommunikationsdaten, z.B. mit der Begründung des berechtigten Interesses, zum anderen Sicherheitspolitiker, die mit unterschiedlichen Begründungen Lücken in den Grundrechtsschutz schlagen wollen.


Bild: iStock.com/imaginima

- Abkürzung: DMA
- Kurzname: Digital Markets Act
- VERORDNUNG (EU) 2022/1925 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. September 2022 über bestreitbare und faire Märkte im digitalen Sektor und zur Änderung der Richtlinien (EU) 2019/1937 und (EU) 2020/1828 (Gesetz über digitale Märkte)
- Stand am 1. Februar 2023: veröffentlicht
- Veröffentlichung: 12. Oktober 2022, ABl. L265/1
- Wirksamkeit: In Kraft 1. November 2022, gilt ab 2. Mai 2023, einige Durchführungsvorschriften bereits ab 1. November 2022
- EP 1. Lesung: 5. Juli 2022
- Ratsentscheidung: 18. Juli 2022
- Legislativvorgang: 2020/0374/COD
- Kommissionsvorschlag COM/2020/767/FINAL vom 16. Dezember 2020

Aus den Erwägungsgründen:

Zweck dieser Verordnung ist es daher, zum reibungslosen Funktionieren des Binnenmarkts beizutragen, indem Vorschriften festgelegt werden, die die Bestreitbarkeit und Fairness der Märkte im digitalen Sektor im Allgemeinen und für gewerbliche Nutzer und Endnutzer zentraler Plattformdienste, die von Torwächtern bereitgestellt werden, im Besonderen gewährleisten. Es sollten geeignete regulatorische Maßnahmen getroffen werden, um gewerbliche Nutzer und Endnutzer der von Torwächtern bereitgestellten zentralen Plattformdienste in der gesamten Union vor unfairen Praktiken von Torwächtern zu schützen, um grenzüberschreitende Geschäfte innerhalb der Union zu erleichtern und auf diese Weise das reibungslose Funktionieren des Binnenmarkts zu verbessern und eine bestehende oder mit Wahrscheinlichkeit entstehende Fragmentierung in den unter diese Verordnung fallenden Bereichen zu beseitigen. Wenngleich Torwächter meist weltweit oder europaweit ausgerichtete Geschäftsmodelle und algorithmische Strukturen zugrunde legen, können sie in verschiedenen Mitgliedstaaten unterschiedliche Konditionen und Geschäftspraktiken anwenden und haben das in einigen Fällen auch getan; dies kann ungleiche Wettbewerbsbedingungen für die Nutzer ihrer zentralen Plattformdienste zur Folge haben, was die Integration des Binnenmarkts beeinträchtigt

Durch eine gewisse Angleichung unterschiedlich gestalteter nationaler Rechtsvorschriften können Hindernisse ausgeräumt werden, die der freien Erbringung und dem freien Empfang von Dienstleistungen wie Einzelhandelsdienstleistungen im Binnenmarkt entgegenstehen. Auf der Ebene der Union sollten daher gezielte harmonisierte rechtliche Verpflichtungen festgelegt werden, um zum Vorteil der Wirtschaft der Union insgesamt und letztlich der Verbraucher in der Union bestreitbare und faire digitale Märkte, auf denen Torwächter tätig sind, im Binnenmarkt sicherzustellen.

EDSB (Europäischer Datenschutzbeauftragter) Stellungnahme vom 10. Februar 2021:

Der EDSB geht in dieser Stellungnahme vor allem auf diejenigen Bestimmungen des Vorschlags ein, die eine sich gegenseitig verstärkende Wettbewerbsfähigkeit des Marktes und letztlich auch Kontrolle der betroffenen Person über ihre personenbezogenen Daten bewirken. (…). Der EDSB formuliert aber auch spezifische Empfehlungen, mit denen sichergestellt werden soll, dass der Vorschlag die DSGVO wirksam ergänzt und den Schutz der Grundrechte und Grundfreiheiten der betroffenen Personen verstärkt und Reibungen mit bestehenden Datenschutzvorschriften vermeidet. (…). Darüber hinaus fordert der EDSB die beiden gesetzgebenden Organe auf, die Aufnahme von Mindestanforderungen an die Interoperabilität für Gatekeeper in Erwägung zu ziehen und die Entwicklung technischer Standards auf europäischer Ebene in Einklang mit den geltenden Rechtsvorschriften der Union über europäische Normung zu fördern. Schließlich empfiehlt der EDSB, unter anderem auf den Erfahrungen mit dem Digital Clearinghouse aufbauend, in Artikel 32 Absatz 1 festzulegen, dass dem Beratenden Ausschuss für digitale Märkte auch Vertreter des EDSA angehören, und fordert ganz allgemein eine institutionalisierte und strukturierte Zusammenarbeit zwischen den einschlägigen zuständigen Aufsichtsbehörden, darunter die Datenschutzbehörden. Mit dieser Zusammenarbeit sollte insbesondere sichergestellt werden, dass alle relevanten Informationen mit den zuständigen Behörden ausgetauscht werden können, damit diese ihre einander ergänzenden Rollen spielen und dabei ihrem jeweiligen institutionellen Auftrag nachkommen können.

- Abkürzung: DSA
- Kurzname: Digital Services Act
- VERORDNUNG (EU) 2022/2065 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG (Gesetz über digitale Dienste)
- Stand am 1. Februar 2023: veröffentlicht
- Veröffentlichung: 27. Oktober 2022, ABl. L277/1
- Wirksamkeit: In Kraft 8. November 2022, gilt ab 17. Februar 2024, Berichtspflichten der Anbieter und Kommissionbefugnisse gelten seit 16. November 2022
- EP 1. Lesung: 5. Juli 2022
- Ratsentscheidung: 4. Oktober 2022
- Legislativvorgang: 2020/0361/COD
- Kommissionsvorschlag COM/2020/825/FINAL vom 16. Dezember 2020

Aus den Erwägungsgründen:

Damit das Online-Umfeld sicher, berechenbar und vertrauenswürdig ist und sowohl Bürgerinnen und Bürger der Union als auch andere Personen die ihnen in der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) garantierten Grundrechte ausüben können, insbesondere das Recht auf Meinungs- und Informationsfreiheit, auf unternehmerische Freiheit, das Recht auf Nichtdiskriminierung und die Erreichung eines hohen Verbraucherschutzniveaus, ist unbedingt ein verantwortungsvolles und sorgfältiges Verhalten der Anbieter von Vermittlungsdiensten erforderlich.

Um das Funktionieren des Binnenmarkts sicherzustellen und zu verbessern, sollten daher auf Unionsebene verbindliche gezielte, einheitliche, wirksame und verhältnismäßige Vorschriften festgelegt werden. Mit dieser Verordnung werden die Voraussetzungen dafür geschaffen, dass im Binnenmarkt innovative digitale Dienste entstehen und expandieren können. Die Angleichung der nationalen Regulierungsmaßnahmen bezüglich der Anforderungen an Anbieter von Vermittlungsdiensten auf Unionsebene ist erforderlich, um eine Fragmentierung des Binnenmarkts zu verhindern und zu beenden, für Rechtssicherheit zu sorgen und somit die Unsicherheit für Entwickler zu verringern und die Interoperabilität zu fördern. Durch die technologieneutrale Gestaltung der Anforderungen sollte die Innovation nicht gehemmt, sondern vielmehr gefördert werden.

EDSB Stellungnahme vom 10. Februar 2021:

Der EDSB begrüßt, dass die im Rahmen der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG bestehenden Schutzmaßnahmen durch den Vorschlag eher ergänzt als ersetzt werden sollen. Unabhängig davon wird sich der Vorschlag eindeutig auf die Verarbeitung personenbezogener Daten auswirken. Der EDSB erachtet es als notwendig, die Komplementarität bei der Überwachung und Beaufsichtigung von Online-Plattformen und anderen Hosting-Diensteanbietern sicherzustellen. Bestimmte Aktivitäten im Zusammenhang mit Online-Plattformen stellen nicht nur für die Rechte Einzelner, sondern für die Gesellschaft als Ganzes zunehmende Risiken dar.

Während der Vorschlag einige Maßnahmen zur Risikominderung enthält, werden zusätzliche Sicherheitsvorkehrungen gewährleistet und dies insbesondere in Bezug auf die Moderation von Inhalten, Online-Werbung und Empfehlungssysteme. Die Moderation von Inhalten sollte nach dem Rechtsstaatlichkeitsprinzip erfolgen. Aufgrund der bereits vorherrschenden Überwachung von Menschen im Internet, insbesondere im Zusammenhang mit Online-Plattformen, sollte das Gesetz über digitale Dienste beschreiben, wann Bemühungen zur Bekämpfung „illegaler Inhalte" die Verwendung automatisierter Mittel zur Erkennung, Feststellung und Bekämpfung illegaler Inhalte rechtfertigen. Das Profiling zum Zwecke der Moderation von Inhalten sollte verboten sein, sofern der Anbieter nicht nachweisen kann, dass diese Maßnahmen unbedingt erforderlich sind, um ausdrücklich durch das Gesetz über digitale Dienste ermittelte systemische Risiken zu bewältigen. Angesichts der Vielzahl von Risiken in Verbindung mit gezielter Online-Werbung drängt der EDSB die Mitgesetzgeber, über die Transparenz hinausgehende zusätzliche Regeln in Betracht zu ziehen. Zu diesen Maßnahmen sollte eine allmähliche Abschaffung gehören, die in einem Verbot von gezielter Werbung auf der Grundlage von allgegenwärtiger Nachverfolgung mündet sowie Beschränkungen in Bezug auf die Datenkategorien, die zu Zwecken der gezielten Ansprache verarbeitet, und die Datenkategorien, die gegenüber Werbetreibenden oder Dritten offengelegt werden dürfen, um gezielte Werbung zu ermöglichen oder zu erleichtern. Entsprechend den Anforderungen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen sollten Empfehlungssysteme nicht grundsätzlich durch Voreinstellung auf Profiling beruhen. Aufgrund ihrer wesentlichen Auswirkungen empfiehlt der EDSB zudem weitere Maßnahmen, um die Transparenz und Nutzerkontrolle in Bezug auf Empfehlungssysteme zu fördern.

Allgemeiner noch empfiehlt der EDSB die Einführung von Mindest-Interoperabilitätsanforderungen für sehr große Online-Plattformen sowie die Förderung der Entwicklung von technischen Normen auf europäischer Ebene gemäß den anwendbaren Rechtsvorschriften der Union im Hinblick auf die europäische Normung. Gestützt auf die Erfahrungen und Entwicklungen im Zusammenhang mit dem Digital Clearinghouse empfiehlt der EDSB nachdrücklich, eine explizite und umfassende Rechtsgrundlage für die Zusammenarbeit und den Austausch relevanter Informationen zwischen den Aufsichtsbehörden, die jeweils im Rahmen ihrer jeweiligen Zuständigkeit handeln, zu schaffen. Das Gesetz über digitale Dienste muss die institutionalisierte und strukturierte Zusammenarbeit zwischen den zuständigen Aufsichtsbehörden einschließlich der Datenschutzbehörden, der Verbraucherschutzbehörden und der Wettbewerbsbehörden sicherstellen.

- Abkürzung: DGA
- Kurzname: Data Governance Act
- Verordnung (EU) 2022/868 des Europäischen Parlaments und des Rates vom 30. Mai 2022 über europäische Daten-Governance und zur Änderung der Verordnung (EU) 2018/1724 (Daten-Governance-Rechtsakt)
- Stand am 1. Februar 2023: veröffentlicht
- Veröffentlichung: 3. Juni 2022 ABl. L152/1
- Wirksamkeit: In Kraft 23. Juni 2022, gilt ab 24. September 2023
- EP 1. Lesung: 6. April 2022
- Ratsentscheidung: 16. Mai 2022
- Legislativvorgang: 2020/0340/COD
- Kommissionsvorschlag COM/2020/767/FINAL vom 25. November 2020

Aus den Erwägungsgründen:

Es ist notwendig, die Bedingungen für die gemeinsame Datennutzung im Binnenmarkt zu verbessern und dazu einen harmonisierten Rahmen für den Datenaustausch zu schaffen sowie bestimmte grundlegende Anforderungen an die Daten-Governance festzulegen, wobei der Erleichterung der Kooperation besondere Aufmerksamkeit zu widmen ist. Ziel dieser Verordnung sollte es sein, die Entwicklung eines grenzfreien digitalen Binnenmarktes sowie eine auf den Menschen ausgerichtete, vertrauenswürdige und sichere Datengesellschaft und -wirtschaft voranzutreiben. Mit sektorspezifischem Unionsrecht, wie beispielsweise dem vorgesehenen Unionsrecht zum europäischen Gesundheitsdatenraum und zum Zugang zu Fahrzeugdaten, können je nach den Besonderheiten eines Sektors neue und ergänzende Elemente entwickelt, angepasst und vorgeschlagen werden. (...) Für die Weiterverwendung geschützter und im Besitz öffentlicher Stellen befindlicher Daten bestimmter

Kategorien sowie für die Erbringung von Datenvermittlungsdiensten und von auf Datenaltruismus beruhenden Diensten in der Union sollte eine horizontale Regelung geschaffen werden. Aufgrund der Besonderheiten verschiedener Sektoren kann es erforderlich sein, ausgehend von den Anforderungen dieser Verordnung sektorale datengestützte Systeme zu konzipieren.

Gemeinsame Stellungnahme 3/2021 des EDSA und des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über europäische Daten-Governance (Daten-Governance-Gesetz), 11. März 2021

Der EDSA und der EDSB weisen darüber hinaus darauf hin, dass das Modell der Europäischen Union auf der durchgängigen Berücksichtigung ihrer Werte und Grundrechte bei den Entwicklungen ihrer Politik beruht und dass die DSGVO als Grundlage betrachtet werden muss, auf der ein europäisches Daten-Governance-Modell aufzubauen ist. Wie bereits in verschiedenen politischen Kontexten, z. B. bei der Bekämpfung der COVID-19-Pandemie, festgestellt wurde, ist der EU-Rechtsrahmen im Bereich des Schutzes personenbezogener Daten als treibende Kraft und nicht als Hindernis für die Entwicklung einer Datenwirtschaft zu betrachten, die den Werten und Grundsätzen der Union entspricht.

- Abkürzung: DA
- Kurzname: Data Act
- Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung (Datengesetz)
- Stand am 1. Februar 2023: 1. Lesung im EP
- Legislativvorgang: 2022/0047(COD)
- Kommissionsvorschlag COM(2022)0068 vom 23. März 2022

Aus der Begründung:

Der Vorschlag für das Datengesetz beinhaltet

- Maßnahmen, damit Nutzer Zugang zu den von ihren vernetzten Geräten erzeugten Daten haben, die häufig ausschließlich von Herstellern gesammelt werden, und diese Daten an Dritte weitergeben können, die anschließende Dienste oder andere datengesteuerte innovative Dienste anbieten. Es bietet nach wie vor Anreize für Hersteller, in eine hochwertige Datenerzeugung zu investieren, weil es ihnen ermöglicht, die durch die Datenweitergabe entstehenden Kosten zu decken, und gleichzeitig ausschließt, dass die von ihnen bereitgestellten Daten verwendet werden, um damit in direkten Wettbewerb zu ihrem Produkt zu treten.
- Maßnahmen zur Wiederherstellung einer ausgewogenen Verhandlungsmacht für KMU durch Verhinderung von Ungleichgewichten in Verträgen über die gemeinsame Datennutzung. Das Datengesetz schützt KMU vor missbräuchlichen Vertragsklauseln, die von einer Vertragspartei mit einer deutlich stärkeren Verhandlungsposition vorgegeben werden. Die Kommission wird auch Mustervertragsbedingungen entwickeln, um KMU dabei zu helfen, faire Verträge über die gemeinsame Datennutzung abzufassen und auszuhandeln.
- Mittel für Behörden für den Zugang zu und die Nutzung von Daten im Besitz des Privatsektors, die unter besonderen Umständen und vor allem bei öffentlichen Notständen wie Überschwemmungen und Waldbränden benötigt werden oder aber zur Wahrnehmung eines rechtlichen Mandats, sofern Daten nicht anderweitig verfügbar sind. Der Datenzugang ist erforderlich, damit rasch und sicher reagiert werden kann und Unternehmen dabei möglichst wenig belastet werden.
- Neue Vorschriften, damit Kunden effektiv wechseln können zwischen Anbietern von Cloud-Datenverarbeitungsdiensten.

und führt Schutzmaßnahmen gegen unrechtmäßige Datenübermittlungen ein.

Gemeinsame Stellungnahme 2/2022 des EDSA und des EDSB zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für den fairen Zugang zu Daten und deren Nutzung, 4. Mai 2022:

While welcoming the efforts made to ensure that the Proposal does not affect the current data protection framework, the EDPB and the EDPS consider that additional safeguards are necessary to avoid lowering the protection of the fundamental rights to privacy and to the protection of personal data in practice. First, additional safeguards are especially necessary as the rights to access, use and share data under the Proposal would likely extend to entities other than the data subjects, including businesses, depending on the legal title under which the device is being used. Second, the EDPB and EDPS are deeply concerned by the provisions of the Proposal regarding the obligation to make data available to public sector bodies and Union institutions, agencies or bodies in case of "exceptional need". Finally, the EDPB and the EDPS are concerned that the oversight mechanism established by the Proposal may lead to fragmented and incoherent supervision.

Übersetzt mit www.DeepL.com/Translator (kostenlose Version):

Der EDSA und der EDSB begrüßen zwar die Bemühungen, die unternommen wurden, um sicherzustellen, dass der Vorschlag den derzeitigen Datenschutzrahmen nicht beeinträchtigt, sind jedoch der Ansicht, dass zusätzliche Garantien erforderlich sind, um zu vermeiden, dass der Schutz der Grundrechte auf Privatsphäre und auf den Schutz personenbezogener Daten in der Praxis beeinträchtigt wird. Erstens sind zusätzliche Garantien vor allem deshalb erforderlich, weil sich die Rechte auf Zugang, Nutzung und Weitergabe von Daten gemäß dem Vorschlag wahrscheinlich auch auf andere Stellen als die betroffenen Personen erstrecken würden, einschließlich Unternehmen, je nachdem, unter welchem Rechtstitel das Gerät verwendet wird. Zweitens sind der EDSA und der EDSB zutiefst besorgt über die Bestimmungen des Vorschlags bezüglich der Verpflichtung, öffentlichen Stellen und Organen, Agenturen oder Einrichtungen der Union im Falle eines „außergewöhnlichen Bedarfs" Daten zur Verfügung zu stellen. Schließlich sind der EDSA und der EDSB

besorgt, dass der durch den Vorschlag eingeführte Aufsichtsmechanismus zu einer fragmentierten und inkohärenten Aufsicht führen könnte.

- Abkürzung: EHDS
- Kurzname: European Health Data Space
- Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über den europäischen Raum für Gesundheitsdaten
- Stand am 1. Februar 2023: EP 1. Lesung
- Legislativvorgang: 2022/0140/COD
- Kommissionsvorschlag COM/2022/197/FINAL vom 4. Mai 2022

Aus der Begründung:

Immer mehr Menschen in Europa überschreiten nationale Grenzen, um zu arbeiten, zu studieren, Verwandte zu besuchen oder zu reisen. Um den Austausch von Gesundheitsdaten zu erleichtern und den Bürgerinnen und Bürgern die benötigte Handlungskompetenz zu verleihen, sollten sie auf ihre Gesundheitsdaten in einem elektronischen Format zugreifen können, das in der gesamten Union anerkannt und akzeptiert werden kann. Solche personenbezogenen elektronischen Gesundheitsdaten könnten personenbezogene Daten über die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdiensten, aus denen Informationen über ihren Gesundheitszustand hervorgehen, personenbezogene Daten zu den ererbten oder erworbenen genetischen Merkmalen einer natürlichen Person, die eindeutige Informationen über den körperlichen Zustand oder die Gesundheit dieser natürlichen Person liefern und speziell das Ergebnis einer Analyse einer Probe von biologischem Material der betreffenden natürlichen Person sind, sowie Datendeterminanten für die Gesundheit wie Verhalten, Umwelt, physische Einflüsse, medizinische Versorgung, soziale Faktoren oder erziehungs-/bildungsbezogene Faktoren umfassen. Elektronische Gesundheitsdaten schließen auch Daten ein, die ursprünglich für Zwecke der Forschung, der Statistik, der Politikgestaltung oder der Regulierung erhoben wurden und nach den Vorschriften in Kapitel IV zur Verfügung gestellt werden können. Die elektronischen Gesundheitsdaten betreffen alle Kategorien dieser Daten, unabhängig davon, ob diese Daten von der betroffenen Person oder anderen natürlichen oder juristischen Personen wie Angehörigen der Gesundheitsberufe bereitgestellt oder im Zusammenhang mit der Gesundheit oder dem Wohlbefinden einer natürlichen Person verarbeitet werden, und sollten auch gefolgerte und abgeleitete Daten, etwa zu Diagnosen, Tests und medizinischen Untersuchungen, sowie automatisch erfasste und aufgezeichnete Daten umfassen.

Die Sekundärnutzung von Gesundheitsdaten im Rahmen des EHDS sollte es öffentlichen, privaten, nicht gewinnorientierten Einrichtungen sowie einzelnen Forschern ermöglichen, für die in der vorliegenden Verordnung festgelegten Zwecke Zugang zu Gesundheitsdaten für Forschung, Innovation, Politikgestaltung, Bildung, Patientensicherheit, Regulierungstätigkeiten oder personalisierte Medizin zu erhalten. Der Zugang zu Daten für die Sekundärnutzung sollte dem allgemeinen Interesse der Gesellschaft dienen.

Zu den Tätigkeiten, für die der Zugang im Rahmen dieser Verordnung rechtmäßig ist, kann die Nutzung elektronischer Gesundheitsdaten durch öffentliche Stellen für die Wahrnehmung ihrer Aufgaben gehören, darunter öffentliche Aufgaben wie Gesundheitsüberwachung, Planung und Berichterstattung, Gestaltung der Gesundheitspolitik sowie Sicherstellung der Patientensicherheit, der Qualität der Versorgung und der Nachhaltigkeit der Gesundheitssysteme. Für öffentliche Einrichtungen und Organe, Einrichtungen und sonstige Stellen der Union kann der regelmäßige Zugang zu elektronischen Gesundheitsdaten über einen längeren Zeitraum erforderlich sein, auch zur Erfüllung ihres Mandats nach Maßgabe dieser Verordnung. Öffentliche Stellen können solche Forschungstätigkeiten unter Einbeziehung von Dritten, einschließlich Unterauftragnehmern, durchführen, solange die öffentliche Stelle jederzeit die Aufsicht über diese Tätigkeiten ausübt.

Mit der Bereitstellung der Daten sollten auch Tätigkeiten unterstützt werden, die mit wissenschaftlicher Forschung (einschließlich privater Forschung), Entwicklung und Innovation oder der Herstellung von Waren und Dienstleistungen für den Gesundheits- oder Pflegesektor zusammenhängen, wie Innovationstätigkeiten oder das Trainieren von KI-Algorithmen, die die Gesundheit natürlicher Personen schützen oder Pflegetätigkeiten unterstützen könnten. In einigen Fällen könnten die Informationen zu bestimmten natürlichen Personen (z. B. Genomdaten natürlicher Personen mit einer bestimmten Krankheit) die Diagnose oder Behandlung anderer natürlicher Personen unterstützen.

Für öffentliche Stellen ist es erforderlich, über den für Notlagen ausgelegten Geltungsbereich von Kapitel V der Verordnung [...] [Datengesetz (COM(2022) 68 final)] hinauszugehen. Die öffentlichen Stellen können jedoch die Stellen für den Zugang zu Gesundheitsdaten um Unterstützung bei der Verarbeitung oder Verlinkung von Daten ersuchen. Die vorliegende Verordnung sieht zwar einen Kanal vor, über den öffentliche Stellen Zugang zu Informationen erhalten können, die sie zur Erfüllung der ihnen gesetzlich übertragenen Aufgaben benötigen, erweitert jedoch nicht das Mandat dieser öffentlichen Stellen. Jedes Bestreben, die Daten für Maßnahmen zum Nachteil der betroffenen natürlichen Person zu verwenden, Versicherungsbeiträge zu erhöhen, Produkte oder Behandlungen zu bewerben oder schädliche Produkte zu entwickeln, sollte verboten werden.

EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space, 12. Juli 2022:

The EDPB and the EDPS note that the provisions in this Proposal will add yet another layer to the already complex (multi-layered) collection of provisions (to be found both in the EU and Member States law) on the processing of health data (in the health care sector). The interplay between those different pieces of legislation needs to be (crystal) clear.

The EDPB and the EDPS also strongly recommend to not extend the scope of

the GDPR exceptions regarding the data subject's rights to the Proposal and in particular in Article 38(2) of the Proposal. Such exemption undermines the possibility for data subjects to exercise an effective control over their personal data rather than strengthen it and thus appears to be at odds with the objective laid down in Article 1(2)(a) of the Proposal.

The EDPB and the EDPS acknowledge the provisions in Chapter III that aim to improve the interoperability of Electronic Health Records and to facilitate the connectivity of wellness-apps with such electronic health records. However, the EDPB and the EDPS are of the opinion that the latter should not be included in the secondary use of health data under Chapter IV of the Proposal. First, because health data generated by wellness applications and other digital health applications do not have the same data quality requirements and characteristics of those generated by medical devices. Moreover, these applications generate an enormous amount of data and can be highly invasive since it relates to every step individuals takes in their everyday lives. Even if health data could be indeed separated from other kinds of data, inferences such as food practices and other habits could be easily made, revealing particularly sensitive information such as religious orientation.

As to the purposes for secondary use of health data listed under Article 34(1) of the Proposal, the EDPB and the EDPS understand that Articles 34(1)(f) and (g) of the Proposal possibly encompass any form of ‚development and innovation activities for products or services contributing to public health or social security' or ‚training, testing and evaluation of algorithms, including in medical devices, AI systems and digital health applications, contributing to public health or social security'. The EDPB and the EDPS are of the view that the Proposal should further delineate these purposes and circumscribe when there is a sufficient connection with public health and/or social security. This will be crucial to achieve a balance adequately taking into account the objectives pursued by the Proposal and the protection of personal data of the data subjects affected by the processing.

Übersetzt mit www.DeepL.com/Translator (kostenlose Version):

Der EDSA und der EDSB stellen fest, dass die Bestimmungen in diesem Vorschlag der bereits komplexen (vielschichtigen) Sammlung von Bestimmungen (die sowohl im EU-Recht als auch im Recht der Mitgliedstaaten zu finden sind) über die Verarbeitung von Gesundheitsdaten (im Gesundheitswesen) noch eine weitere Ebene hinzufügen werden. Das Zusammenspiel zwischen diesen verschiedenen Rechtsakten muss (kristallklar) sein. [...]

- Abkürzung: AIA
- Kurzname: Artificial Intelligence Act
- Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES ZUR FESTLEGUNG HARMONISIERTER VORSCHRIFTEN FÜR KÜNSTLICHE INTELLIGENZ (GESETZ ÜBER KÜNSTLICHE INTELLIGENZ) UND ZUR ÄNDERUNG BESTIMMTER RECHTSAKTE DER UNION
- Stand am 1. Februar 2023: 1. Lesung im EP, informelle Verhandlung mit dem Rat
- Legislativvorgang: 2021/0106/COD
- Kommissionsvorschlag COM/2021/206/FINAL vom 22. April 2021

Aus der Begründung:

Künstliche Intelligenz bezeichnet eine Reihe von Technologien, die sich rasant entwickeln und zu vielfältigem Nutzen für Wirtschaft und Gesellschaft über das gesamte Spektrum industrieller und gesellschaftlicher Aktivitäten hinweg beitragen können. Durch die Verbesserung der Vorhersage, Optimierung der Abläufe, Ressourcenzuweisung und Personalisierung digitaler Lösungen, die Einzelpersonen und Organisationen zur Verfügung stehen, kann die Verwendung künstlicher Intelligenz den Unternehmen wesentliche Wettbewerbsvorteile verschaffen und zu guten Ergebnissen für Gesellschaft und Umwelt führen, beispielsweise in den Bereichen Gesundheitsversorgung, Landwirtschaft, allgemeine und berufliche Bildung, Infrastrukturmanagement, Energie, Verkehr und Logistik, öffentliche Dienstleistungen, Sicherheit, Justiz, Ressourcen- und Energieeffizienz sowie Klimaschutz und Anpassung an den Klimawandel.

Gleichzeitig kann künstliche Intelligenz je nach den Umständen ihrer konkreten Anwendung und Nutzung Risiken mit sich bringen und öffentliche Interessen und Rechte schädigen, die durch das Unionsrecht geschützt sind. Ein solcher Schaden kann materieller oder immaterieller Art sein.

Daher ist ein Rechtsrahmen der Union mit harmonisierten Vorschriften für künstliche Intelligenz erforderlich, um die Entwicklung, Verwendung und Verbreitung künstlicher Intelligenz im Binnenmarkt zu fördern und gleichzeitig einen hohen Schutz öffentlicher Interessen wie Gesundheit und Sicherheit und den Schutz der durch das Unionsrecht anerkannten und geschützten Grundrechte zu gewährleisten. Zur Umsetzung dieses Ziels sollten Vorschriften für das Inverkehrbringen und die Inbetriebnahme bestimmter KI-Systeme festgelegt werden, um das reibungslose Funktionieren des Binnenmarkts zu gewährleisten, sodass diesen Systemen der Grundsatz des freien Waren- und Dienstleistungsverkehrs zugutekommen kann. Durch die Festlegung dieser Vorschriften unterstützt die Verordnung das vom Europäischen Rat formulierte Ziel der Union, bei der Entwicklung einer sicheren, vertrauenswürdigen und ethisch vertretbaren künstlichen Intelligenz weltweit eine Führungsrolle einzunehmen, und sorgt für den vom Europäischen Parlament ausdrücklich geforderten Schutz von Ethikgrundsätzen.

EDSA-EDSB Gemeinsame Stellungnahme 5/2021 zum Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Gesetz über künstliche Intelligenz) und zur Änderung bestimmter Rechtsakte der Union, 18. Juni 2021:

Der EDSA und der EDSB stellen fest, dass die Rechtsgrundlage für den Vorschlag in erster Linie Artikel 114 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ist. Darüber hinaus beruht der Vorschlag auch auf Artikel 16 AEUV, insofern er spezifische

Regeln über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten enthält, vor allem Einschränkungen der Verwendung von KI-Systemen zur biometrischen Fernidentifizierung in Echtzeit in öffentlich zugänglichen Räumen für die Zwecke der Strafverfolgung. Der EDSA und der EDSB erinnern daran, dass Artikel 16 AEUV nach der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) eine geeignete Rechtsgrundlage darstellt, wenn der Schutz personenbezogener Daten eines der wesentlichen Ziele oder Komponenten der vom Unionsgesetzgeber erlassenen Regeln ist. Mit der Anwendung von Artikel 16 AEUV geht, was die Anforderungen an die Verarbeitung personenbezogener Daten betrifft, das Erfordernis einher, die Überwachung der Einhaltung der Regeln durch eine unabhängige Stelle sicherzustellen, was auch nach Artikel 8 der Charta der Grundrechte der Europäischen Union erforderlich ist. Die biometrische Fernidentifizierung natürlicher Personen in öffentlich zugänglichen Räumen birgt ein hohes Risiko, dass die Privatsphäre natürlicher Personen verletzt wird, und läuft der Erwartung der Bevölkerung, im öffentlichen Raum anonym zu bleiben, fundamental zuwider. Aus diesen Gründen erheben der EDSA und der EDSB die Forderung nach einem allgemeinen Verbot der Verwendung von KI zur automatischen Erkennung von personenbezogenen Merkmalen in öffentlich zugänglichen Räumen, und zwar in jeglichem Zusammenhang; solche Merkmale sind z. B. Gesichtszüge, aber auch Gangart, Fingerabdrücke, DNA, Stimme, Tastenanschlagsmuster und andere biometrische Merkmale oder Verhaltenssignale.

Der EDSA und der EDSB begrüßen die Benennung des EDSB als die zuständige Behörde und Marktüberwachungsbehörde für die Aufsicht über die Organe, Einrichtungen und sonstigen Stellen der Union. Die Rolle und die Aufgaben des EDSB sollten jedoch genauer spezifiziert werden, vor allem in Bezug auf seine Rolle als Marktüberwachungsbehörde. Des Weiteren sollte in der künftigen KI-Verordnung die Unabhängigkeit der Aufsichtsbehörden in der Wahrnehmung ihrer Aufsichts- und Durchsetzungsaufgaben klargestellt werden. Die Benennung der Datenschutzbehörden (DSB) als nationale Aufsichtsbehörden würde einen einheitlicheren Regulierungsansatz ermöglichen und dazu beitragen, dass die Mitgliedstaaten die Datenverarbeitungsvorschriften einheitlich auslegen und Widersprüche in deren Durchsetzung vermeiden. Der EDSA und der EDSB sind deshalb der Auffassung, dass die Datenschutzbehörden als zuständige nationale Aufsichtsbehörden im Sinne von Artikel 59 des Vorschlags benannt werden sollten.

- Abkürzung: ePR
- Kurzname: ePrivacy Regulation
- Vorschlag für eine VERORDNUNG DES EUROPÄISCHEN PARLAMENTS UND DES RATES über die Achtung des Privatlebens und den Schutz personenbezogener Daten in der elektronischen Kommunikation und zur Aufhebung der Richtlinie 2002/58/EG (Verordnung über Privatsphäre und elektronische Kommunikation)
- Stand am 1. Februar 2023: Informelle Verhandlungen zwischen EP und Rat, seit 2021
- Legislativvorgang: 2017/0003(COD)
- Kommissionsvorschlag: COM/2017/10/FINAL vom 11. Januar 2017

Aus den Erwägungsgründen:

Die e-Privacy-Richtlinie gewährleistet den Schutz von Grundrechten und Grundfreiheiten, insbesondere die Achtung des Privatlebens, die Wahrung der Vertraulichkeit der Kommunikation und den Schutz personenbezogener Daten im Bereich der elektronischen Kommunikation. Außerdem gewährleistet sie den freien Verkehr von elektronischen Kommunikationsdaten, -geräten und -diensten in der Union. Sie bewirkt hinsichtlich der Kommunikation die Umsetzung des in Artikel 7 der Charta der Grundrechte der Europäischen Union („Charta") verankerten Grundrechts auf Achtung des Privatlebens im Sekundärrecht der Union.

Die e-Privacy-Richtlinie ist Teil des Rechtsrahmens für die elektronische Kommunikation. Im Jahr 2016 nahm die Kommission den Vorschlag für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation („Kodex") an, mit dem der Rechtsrahmen überarbeitet wird. Der vorliegende Vorschlag ist zwar kein Bestandteil des Kodex, er beruht aber teilweise auf darin enthaltenen Begriffsbestimmungen wie der für „elektronische Kommunikationsdienste". Wie der Kodex erfasst auch der vorliegende Vorschlag OTT-Anbieter in seinem Anwendungsbereich, um der Marktwirklichkeit Rechnung zu tragen. Überdies ergänzt der Kodex diesen Vorschlag, indem er die Sicherheit elektronischer Kommunikationsdienste gewährleistet.

Empfehlungen des EDSB zu bestimmten Aspekten der vorgeschlagenen Verordnung über Privatsphäre und elektronische Kommunikation, 5. Oktober 2017:

Die Verordnung über Privatsphäre und elektronische Kommunikation sollte die Bedeutung des Grundsatzes der Vertraulichkeit der Kommunikation verdeutlichen, der eng mit dem Recht auf Privatleben verknüpft ist und somit durch die EU-Charta der Grundrechte, die Europäische Menschenrechtskonvention sowie die Verfassungs- und Rechtsordnungen der meisten Mitgliedstaaten geschützt ist. Unter die Vertraulichkeit der Kommunikation fallen sowohl Inhaltsdaten und Metadaten als auch Endeinrichtungen betreffende Daten. Dies sollte seinen angemessenen Ausdruck in den erlaubten Zwecken der Verarbeitung und in den Rechtsgrundlagen der Verarbeitung finden. Diese Erwägungen beziehen sich auf alle Bestimmungen der Verordnung über Privatsphäre und elektronische Kommunikation.

Die Verordnung über Privatsphäre und elektronische Kommunikation sollte einen echten Schutz im Einklang mit bestehenden und künftig zu erwartenden technologischen Entwicklungen bieten, insbesondere mit Blick auf Maschine-zu-Maschine-Kommunikation. Insofern unterstützen wir Änderungsanträge, die ausdrücklich den Schutz der Vertraulichkeit der Kommunikation für „Daten" fordern, „die im Zusammenhang mit Endgeräten stehen oder von diesen verarbeitet werden". Die Vertraulichkeit der Kommunikation sollte ferner gewährleistet sein, wenn Daten in der

Cloud gespeichert werden, und nicht nur bei der Übermittlung.

Der Ansatz, demzufolge die Verordnung über Privatsphäre und elektronische Kommunikation die Datenschutz-Grundverordnung spezifiziert und ergänzt, sollte beibehalten werden, um die Bedeutung der Vertraulichkeit der Kommunikation zu unterstreichen. Die Verordnung über Privatsphäre und elektronische Kommunikation sollte das in der Datenschutz-Grundverordnung vorgesehene Schutzniveau keinesfalls senken. Vielmehr sollte ein höheres Schutzniveau als das in der Datenschutz-Grundverordnung vorgesehene geboten werden. Gleichzeitig sollten im Sinne von Klarheit und Rechtssicherheit unnötige Wiederholungen von Bestimmungen der Datenschutz-Grundverordnung vermieden werden; werden selektiv nur einige Bestimmungen der Datenschutz-Grundverordnung wiederholt, besteht die Gefahr, dass wichtige Bestimmungen dabei nicht erfasst werden.

Eine breit angelegte Rechtsgrundlage für die Verarbeitung von Kommunikationsdaten durch Verweis auf die Datenschutz-Grundverordnung oder durch Zitieren der Datenschutz-Grundverordnung wäre der Begründung eines spezifischen Rechtsinstruments abträglich und würde der Bedeutung des Grundsatzes der Vertraulichkeit der Kommunikation nicht angemessen gerecht, wie er sowohl in der Charta der Grundrechte als auch in der Rechtsprechung von EuGH und EGMR verankert ist. So sollte nach der Verordnung über Privatsphäre und elektronische Kommunikation auf keinen Fall die Möglichkeit einer Verarbeitung von Metadaten aus Gründen des berechtigten Interesses gegeben sein. Die Erlaubnis einer Verarbeitung aus Gründen des berechtigten Interesses würde die heute gemäß der Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG anzuwendenden Standards spürbar senken und den Mehrwert des Verordnungsentwurfs in Frage stellen. In ähnlicher Weise würde die Weiterverarbeitung von Metadaten ein Schlupfloch schaffen und ein Umgehen des hohen Schutzniveaus ermöglichen. Endgeräte betreffende Daten sollten nur nach Einwilligung oder in Fällen verarbeitet werden, in denen dies für einen vom Nutzer verlangten Dienst erforderlich ist, und dann auch nur so lange, wie es für diesen Zweck erforderlich ist. Wir unterstützen daher Änderungsanträge, die die breit angelegte Rechtsgrundlage für das Tracking natürlicher Personen über Zeit und Raum zu allen Zwecken streichen.

Eric Hilgendorf

Datenschutz und Datenhandel – Friktionen in der europäischen Digitalpolitik*

I. Einleitung

Glaubt man der Europäischen Kommission, so befinden wir uns auf dem „Weg ins digitale Jahrzehnt“. Seit dem Frühjahr 2020 bringt die EU in hohem Tempo immer neue Rechtsakte zur Regulierung der digitalen Transformation auf den Weg, wobei häufig auf die von der „High Level Expert Group on AI“ erarbeiteten Standards Bezug genommen wird.[1] Zu den wichtigsten Neuerungen gehören der „Digital Markets Act“[2], der „Digital Services Act“[3], der Entwurf einer KI-Verordnung[4] und zuletzt der überaus ambitionierte Vorschlag zu einem neuen „Data Act“[5]. Ziel der EU ist es einen belastbaren Rechtsrahmen für die Digitale Transformation in Europa zu schaffen, Sicherheit in den Netzen zu gewährleisten und gleichzeitig den Übergang vom traditionellen „Datenschutz“ zur gemeinwohlfördernden „Datennutzung“ in die Wege zu leiten.[6]

Zu den genannten großen Rechtsakten tritt noch eine Vielzahl kleiner Regulierungen und Regulierungsvorschläge hinzu. Eine aktuelle Übersicht auf einer Internetseite des Europäischen Parlaments zählt sage und schreibe 101 solcher Rechtsakte auf.[7] Selbst für Spezialistinnen und Spezialisten ist es kaum möglich, hier noch einen Überblick zu behalten, zumal sich die Regelungsvorschläge auf sämtliche Rechtsgebiete erstrecken. Es kommt zu offenkundigen Überschneidungen, gelegentlich auch zu Widersprüchen, die sich teilweise zwischen den Entwürfen ergeben, mehr aber noch im Verhältnis zu älteren EU-Regelungen. So ist etwa unklar, wie sich die Vorschriften im Entwurf der neuen KI-Verordnung über Hochrisiko-KI-Systeme mit dem überkommenen EU-Produkthaftungsrecht vereinbaren lassen sollen.[8] Meine Vermutung geht dahin, dass selbst die gesetzesvorbereitenden Kommissionsmitarbeiterinnen und -mitarbeiter nicht immer ihre Vorschläge hinreichend aufeinander abstimmen.

Über die Gründe für dieses hohe – viele würden sagen: zu hohe – Tempo kann man nur spekulieren. Eine Erklärung könnte sein, dass es die Kommission vermeiden möchte, von den großen Digitalkonzernen weiterhin vor vollendete Tatsachen gestellt zu werden. Dazu passt, dass immer wieder hochrangige Kommissionsmitarbeiter oder sogar Mitglieder der Kommission selbst mit der Aussage zitiert werden, es ginge darum, Internet und Datenwirtschaft endlich gemeinwohlverträglich zu regulieren.[9]

Die Entwürfe haben nach meinem Eindruck ganz überwiegend ein hohes Niveau und könnten tatsächlich dazu beitragen, die Digitalwirtschaft in Europa in einer grundrechtssensitiven, verbraucherfreundlichen und gemeinwohlorientierten Weise zu regulieren. Dennoch führt das Tempo, in welchem die Regulierungsvorhaben aufeinander-

folgen, wie nicht anders zu erwarten, zu teilweise erheblichen Friktionen. Besonders problemträchtig, und das ist das Thema, zu dem ich heute vor Ihnen sprechen darf, ist die deutliche Spannung, die zwischen der Datenschutz-Grundverordnung und neuen gesetzgeberischen Vorstößen in Richtung auf die Schaffung einer europäischen Datenökonomie besteht.

II. Überblick über die neuen Rechtsakte

Im Data Governance Act, vorgestellt am 25. November 2020 und am 23.06.2022 in Kraft getreten, geht es darum, die Verfügbarkeit und den Austausch von Daten als dem „Öl des 21. Jahrhunderts" zwischen Privatpersonen, Unternehmen und der öffentlichen Hand zu erleichtern. Daten aus Bereichen wie Agrarwirtschaft, Gesundheit, Mobilität und Umwelt sollen effektiver für das Gemeinwohl genutzt werden. Dies betrifft nicht bloß wirtschaftliche Effizienz und Wertschöpfung, sondern auch den Einsatz von Daten in Forschung und Innovation, ein Gesichtspunkt, dessen große Bedeutung die Corona-Pandemie unübersehbar vor Augen geführt hat. In der Verordnung werden neue Akteure, etwa neutrale Datentreuhänder und Datenmittler, definiert. Im Data Governance Act wird des Weiteren die Möglichkeit einer Datenspende, also die freiwillige Bereitstellung von Daten durch einzelne Personen oder Unternehmen zur Förderung des Gemeinwohls, behandelt. In diesem Zusammenhang sollen auch sogenannte „datenaltruistische Organisationen" entstehen, welche den freien Fluss der Daten fördern.

Im Digital Services Act (DSA) vom 15. Dezember 2020[10] geht es im Kern darum die großen Internetanbieter, insbesondere die Anbieter von Online-Plattformen und sozialen Medien, stärker in die Pflicht zu nehmen, indem ihnen unter anderem detaillierte Sorgfalts- und Rechenschaftspflichten auferlegt werden. Dazu knüpft der DSA an das deutsche Netzwerkdurchsetzungsgesetz an und bildet es fort. Plattformbetreiber werden verpflichtet, Transparenz zu schaffen, Nutzern Widerspruchsmöglichkeiten zu geben, zügig gegen rechtswidrige Inhalte vorzugehen und besser mit den staatlichen Behörden zu kooperieren.

Zusammen mit dem Digital Services Act wurde am 15. Dezember 2020 auch der Vorschlag für eine Verordnung über „faire Märkte im digitalen Sektor" (Digital Markets Act, DMA) publiziert.[11] Ziel dieses Rechtsaktes ist es, mehr Wettbewerb auf den europäischen digitalen Märkten zu sichern. Dazu wird als neues Konzept der sog „Gatekeeper" eingeführt. Gatekeeper ist nach Art. 3 Abs. 1 DMA jeder Betreiber eines zentralen Plattformdienstes (Art. 1 Abs. 2 DMA), der erhebliche Auswirkungen auf den Binnenmarkt hat, gewerblichen Nutzern als Zugangstor zu Endnutzern dient und der hinsichtlich seiner Tätigkeiten eine gefestigte und dauerhafte Position innehat oder absehbar in Kürze erlangen wird. Letztlich geht es also um Plattform-Unternehmen mit besonders großer Marktmacht. In Art. 3 Abs. 2 DMA werden quantitative Kriterien aufgestellt (45 Millionen Endnutzer bzw. 10.000 gewerbliche Nutzer in der EU). Besonders einschneidend ist die Festlegung des Digital Market Acts, dass Gatekeeper Daten unterschiedlicher Onlinedienste nicht mehr kombinieren dürfen. Dies bedeutet unter anderem, dass Regeln für Instagram, WhatsApp und Facebook neu gestaltet werden müssten. In ähnlicher Weise sind auch andere Gatekeeper wie Microsoft, Google, Apple und Amazon betroffen.

Der Entwurf eines Artificial Intelligence Act (AIA) vom 21. April 2021[12] sieht vor, KI-Technologie in Risikoklassen zu unterteilen. Besonders gefährliche Technologien, etwa solche, die zur unbewussten Beeinflussung von Menschen eingesetzt werden könnten, werden verboten. In eine zweite Kategorie fallen sogenannte Hochrisiko-Technologien, etwa KI-Systeme, die im Bereich der Bewerberauswahl, in Strafverfahren, im Straßenverkehr oder für Grenzkontrollen eingesetzt werden sollen. Der Einsatz derartiger Technologien ist zwar zulässig, wird aber detailliert reguliert. Dagegen gelten für weniger gefährliche bzw. ungefährliche KI-Technologien lediglich Transparenzpflichten. Bemerkenswert am AI Act ist das sehr weite Verständnis von Künstlicher Intelligenz, das dazu führen könnte, dass große Teile der Digitaltechnik dem AI Act unterfallen. Ergänzt wird der AI Act durch die neuen Vorschläge für ein modernisiertes KI-Haftungsrecht.[13]

Zu nennen ist schließlich auch der Entwurf eines Data Act vom 23. Februar 2022,[14] der ähnlich wie der Data Governance Act den Zugang und Handel mit Daten erleichtern soll. Dazu wurde im Februar 2022 auch ein Vorschlag zu einer methodologischen Analyse der Datenströme in der EU publiziert.[15] Ziel des Data Acts ist es, Datensilos aufzubrechen und so ein innovations- und handelsfreundliches Umfeld für die Wertschöpfung aus Daten zu ermöglichen. Auch im Data Act finden sich Regelungen gegen sog. „Gatekeeper".

Juristisch geht es in den genannten Rechtsakten um die Weiterentwicklung des tradierten Datenschutzrechtes zu einem allgemeinen Datenrecht; wirtschaftlich um die Realisierung der mit Daten heute denkbaren Wertschöpfung und politisch um das Aufbrechen von „Datensilos" und die Einhegung der Tech-Giganten, welche die weitgehend unregulierte Datenlandschaft der vergangenen zwei Jahrzehnte dazu genutzt haben ungeheure Reichtümer aufzuhäufen und Quasi-Monopole zu errichten, deren politische und wirtschaftliche Gefahren mittlerweile immer deutlicher werden.[16]

Will man die skizzierte Entwicklung auf eine knappe Formel bringen, so könnte man sagen, dass das tradierte Datenschutzrecht zu einem allgemeinen europäischen Datenrecht weiterentwickelt werden soll.[17] Die potentiell weit über Europa hinausreichende Wirksamkeit der neuen Rechtsakte wird von der Kommission durchaus erkannt und offen ausgesprochen. Dahinter steht das Phänomen des „Brussels Effect", der sich daraus ergibt, dass US-Konzerne, um auf dem Europäischen Markt erfolgreich zu sein, rechtliche EU-Vorgaben häufig bei ihren Geschäftsmodellen und der Gestaltung ihrer Produkte berücksichtigen.[18] Der „Brussels Effect" beruht also auf ökonomischem Kalkül, nicht unbedingt auf Anerkennung einer Überlegenheit der Europäischen Gesetzgebung. Die gegenwärtigen politischen und ökonomischen Entwicklungen, die die Stellung der USA gegenüber Europa erheblich verstärkt haben und wohl auch noch weiter verstärken werden, dürften dazu beitragen, den „Brussels Effect" deutlich abzuschwächen.

Künftig lassen sich drei große Teilbereiche des Datenrechtes unterscheiden: das Datenwirtschaftsrecht, in dem es um die Verfügbarkeit und den Handel mit Daten geht, das traditionelle Datenschutzrecht, welches den Schutz des Rechts auf informationelle Selbstbestimmung regelt und daher den Umgang mit Daten einschränkt, und schließlich das Internet- und Datenstrafrecht.[19] Im Folgenden sollen nur die ersten beiden Bereiche des Datenrechts, also das Datenwirtschaftsrecht und das Datenschutzrecht, angesprochen werden.

III. Das klassische Datenschutzrecht

Datenschutz ist Grundrechtsschutz. Geschützt wird das Recht auf informationelle Selbstbestimmung, welches vom Bundesverfassungsgericht in seinem berühmten Volkszählungsurteil[20] aus der Menschenwürde und dem Grundrecht auf allgemeine Handlungsfreiheit hergeleitet wurde.

In diesem Urteil wurden auch die bis heute gültigen Grundsätze des Datenschutzrechtes entwickelt. „Nach diesen Grundsätzen", so formuliert es Rossnagel, „ist jeder Umgang mit personenbezogenen Daten ein Eingriff in das Grundrecht auf informationelle Selbstbestimmung. Er soll daher soweit möglich vermieden werden. Zulässig ist er nur, wenn der Gesetzgeber durch einen Erlaubnistatbestand oder der Betroffene durch seine Einwilligung ihn hinsichtlich Umfang und Zweck gebilligt haben. Er muss dem Betroffenen gegenüber durch Unterrichtung, Benachrichtigung oder Auskunft transparent gemacht werden, um ihm die Überprüfung der Rechtmäßigkeit und die Geltendmachung seiner Mitwirkungsrechte zu ermöglichen. Der Umgang mit den Daten ist auf den gebilligten Zweck beschränkt und darf nur so weit und so lange erfolgen, wie dies für die Erreichung dieses Zwecks erforderlich ist. Diese Grundsätze sind durch technisch-organisatorische Maßnahmen abzusichern. Dem Betroffenen stehen Mitwirkungsrechte und Rechte auf Schadensersatz zu."[21]

Diese Grundsätze stehen offenkundig in Widerspruch zu wesentlichen Zielsetzungen der neuen EU-Datengesetze: Einerseits geht es um den Schutz ganz bestimmter, nämlich personenbezogener Daten, andererseits um das Verfügbarmachen und den Handel mit Daten, wobei die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten offenbar keine entscheidende Rolle mehr spielen soll. Dasselbe gilt für den Grundsatz der Datensparsamkeit – bei „Big Data" geht es ganz im Gegenteil darum, möglichst viele Daten zu erheben und zu speichern. Und auch der Grundsatz der Zweckbindung passt nicht zur neuen ökonomischen Betrachtungsweise; vielmehr sind Daten umso wertvoller, desto umfassender und vielfältiger sie sich auswerten und zur Wertschöpfung einsetzen lassen.

Über die neuen EU-Regularien hinaus steht der Datenschutz vor noch weiteren Herausforderungen. Ein Kernproblem des deutschen Datenschutzes besteht seit jeher darin, dass sich US-Konzerne eher widerwillig an deutsche Datenschutzvorgaben halten. Bei Europäischen Datenschutzvorgaben sieht dies offenbar anders aus – der „Brussels Effect" wurde bereits erwähnt. Die Datenschutz-Grundverordnung (DSGVO) hat sich entgegen den Erwartungen vieler Beobachter in wenigen Jahren zu einer Art internationalem „Goldstandard" des Datenschutzes entwickelt. Allerdings sind die Regeln zum Datenschutz heute zu komplex; es kündigt sich eine Entwicklung ähnlich wie im Steuerrecht an, das so kompliziert ist, dass es rechtsstaatlichen Anforderungen kaum mehr genügt. Datenschutz-Grundverordnung, Bundesdatenschutzgesetz und zahlreiche Landesgesetze überschneiden sich in einer selbst für Experten nicht immer durchsichtigen Weise.

Problematisch ist auch die Vielzahl der Vollzugsdefizite; es dürfte kein Rechtsgebiet geben, bei dem eine vergleichbare Kluft zwischen den gesetzlichen Vorgaben und der Realität besteht. Nicht unproblematisch ist ferner die mangelnde Akzeptanz des Datenschutzes in der Bevölkerung. Die Mehrzahl der Bürgerinnen und Bürger nimmt vom Datenschutz allenfalls oberflächlich Kenntnis. Es wäre deshalb fatal, wenn im Datenschutzrecht, in Kombination mit dem neuen Datenwirtschaftsrecht, eine Entwicklung fortgeführt würde, die auf mittlere Sicht die Gesellschaft vom Schutz der informationellen Selbstbestimmung entfremden könnte. Datenschutz ist nicht nur für das Individuum nach wie vor von überragender Bedeutung,[22] sondern besitzt auch eine besondere politische Dimension, eine Bedeutung für Demokratie und Gemeinwohl, wie sie sonst wohl nur der Meinungsfreiheit zukommt. Herrschaft über die Daten der Bürgerinnen und Bürger bedeutet politische Macht. Die Gefahren gehen heute allerdings weniger vom Staat als vielmehr von privaten, demokratisch kaum mehr kontrollierbaren Mega-Konzernen aus.[23]

Auch wenn Datenschutz grundsätzlich bejaht wird, steht die eigene Lebenspraxis dazu doch oft in erheblichem Widerspruch. Ein Stichwort ist das sogenannte „Privacy-Paradox" – einerseits fordern wir Datenschutz, andererseits gehen wir mit unseren Daten selbst oft extrem sorglos um. Ein weiteres, kaum thematisiertes Problem sind Aktivisten, die sich einem absoluten Datenschutz verschrieben haben und echte oder vermeintliche Verstöße gegen den Datenschutz erbittert verfolgen. Gelegentlich geht dies so weit, dass der Verdacht entsteht, es handele sich um bewusst karikierende Übertreibungen, um den Datenschutz in der öffentlichen Meinung zu beschädigen.[24] Häufig wird dabei verkannt, dass datenschutzrechtliche Vorgaben (fast) stets auch Ausnahmen kennen und der Abwägung zugänglich sind. Man könnte von einem fehlgeleiteten „Datenschutzabsolutismus" sprechen, der vor allem in der Pandemie eine teilweise überaus problematische Rolle spielte.

Datenschutz ist, um es noch einmal zu betonen, Grundrechtsschutz. Damit ist ein Datenschutzabsolutismus von vornherein nicht vereinbar. Für das Datenschutzrecht gilt der Verhältnismäßigkeitsgrundsatz, der besagt, dass auch Grundrechte eingeschränkt werden können, wenn ein legitimes Ziel verfolgt, und die einschränkenden Maßnahmen zur Verfolgung des Zieles geeignet, erforderlich und außerdem angemessen sind. In der Corona-Pandemie scheint die im Verhältnismäßigkeitsgrundsatz begründete Flexibilität und Anpassungsfähigkeit des Datenschutzes von nicht wenigen Aktivisten und leider auch Politikern übersehen worden zu sein.

Ein weiteres Problem liegt darin, dass der Unterschied zwischen personenbezogenen und nicht personenbezogenen Daten mit dem technischen Fortschritt zunehmend problematisch geworden ist. Personenbezogen sind Daten auch dann, wenn sie zwar nicht unmittelbar, aber doch mit einem vertretbaren technischen Aufwand auf eine konkrete Person bezogen werden können. Mit dem technischen Fortschritt, der u.a. die Leistungsfähigkeit von Rechnern immer weiter erhöht, wird die Menge der Daten, die grundsätzlich mit einer bestimmten Person in Verbindung gebracht werden kann, fortwährend größer. Dies hängt auch damit zusammen, dass immer mehr Daten erhoben, gespeichert und daher auch miteinander verknüpft werden können, um bestimmte Personen zu identifizieren. Es erscheint denkbar, dass die Unterscheidung zwischen personenbezogenen und nicht personenbezogenen Daten in wenigen Jahren obsolet werden könnte.[25]

Die neuen EU-Vorgaben, gerade der Data Act, lassen die skizzierten Probleme und Entwicklungen in einem besonders hellen Licht erscheinen. Einerseits strebt die EU eine zukunftsgerichtete Regulierung an, die die Verwertung von Daten zugunsten der Wirtschaft und des gemeinen Wohls erleichtern oder sogar erst ermöglichen soll. Andererseits droht gerade der Data Act den Datenschutz zu relativieren und im schlimmsten Falle auszuhöhlen. Es lohnt sich deshalb, den neuen Rechtsakt etwas näher zu betrachten.

IV. Die neuen Rechtsakte der EU

Daten besitzen heutzutage nicht bloß mit Blick auf das Recht auf informationelle Selbstbestimmung Bedeutung, sondern haben auch einen unter Umständen enormen wirtschaftlichen Wert. Sie sind, so sagt man häufig, das Öl des 21. Jahrhunderts. Der Vergleich passt nicht ganz, denn anders als Öl werden Daten durch ihre Verwendung nicht aufgebraucht, sondern stehen weiteren Verwendungsmöglichkeiten offen. Das steigert ihren Wert aber nur noch. Ihnen kommt deshalb eine ganz besondere Bedeutung auch und gerade für das Gemeinwohl zu. Der mit ihnen erwirtschaftete Wohlstand kann Arbeitsplätze sichern, hilft dabei, das Gesundheitssystem und den Sozialstaat zu finanzieren, und dient so indirekt dem Wohlergehen, der Gesundheit und der Verbesserung der Lebenschancen zahlloser Menschen.

Diese neue Bedeutung besitzen nicht bloß personenbezogene, sondern auch und vielleicht sogar gerade nicht personenbezogene Daten, etwa Daten, die in modernen Produktionsmaschinen oder in PKWs entstehen. Die Europäische Union versucht mit ihren neuen Rechtsakten, insbesondere dem Data Act, diesen wirtschaftlichen Wert zu heben, indem sie die Voraussetzungen einer europaweiten Datenökonomie, eines digitalen Binnenmarkes, zu definieren versucht. Dabei wird wie schon erwähnt durchaus auch eine Wirkung über die europäischen Grenzen hinaus angestrebt.[26] Die Zielsetzung des Entwurfs zu einem Europäischen „Datengesetz“ (Data Act) lässt sich am besten durch ein Beispiel verdeutlichen:

Anders als früher sind heute in einem PKW zahlreiche Sensoren verbaut, die gewaltige Datenmengen aufnehmen können. Solche Daten beziehen sich nicht bloß auf traditionelle Faktoren wie die Zahl der gefahrenen Kilometer oder die erreichte Höchstgeschwindigkeit, sondern können auch etwa die Belastung von Bremsen relativ zu gefahrenen Kilometern und zur gefahrenen Geschwindigkeit oder Besonderheiten der Fahrweise relativ zur befahrenen Strecke erfassen. Es liegt auf der Hand, dass etwa die Daten über die Belastung der Bremsen für die Hersteller von Bremsanlagen einen beträchtlichen ökonomischen Wert darstellen, ebenso für Unternehmen, die die Bremsen warten oder reparieren.

Wer darf über diese Daten verfügen? Juristische Laien sind oft der Meinung, mit dem Eigentum am Fahrzeug gehe auch das Eigentum an den darin erzeugten Daten einher. Diese Ansicht ist jedoch schon deshalb irrig, weil Daten mangels Körperlichkeit gar nicht eigentumsfähig sind. Ein Eigentum an Daten gibt es (noch?) nicht.[27] Es verstößt deshalb nicht gegen Rechte des Fahrzeug-Eigentümers, wenn der Hersteller etwa im Rahmen der Wartung oder aber auch per Funk die angesprochenen technischen Daten abzieht und dafür verwendet, seine Produktion zu verbessern. Ähnliches ist heute Alltagspraxis. Allerdings wird man fragen dürfen, ob es in einer sozialen Marktwirtschaft nicht angemessen wäre, den Eigentümer an der Wertschöpfung mit „seinen“ Daten zu beteiligen. Diese Frage wurde von einem Teil des Schrifttums so beantwortet, dass die Schaffung eines echten Dateneigentums gefordert wurde. Ein solches Eigentum an den Daten ließe sich dann etwa dem Fahrzeugkäufer zusprechen, der sodann mit dem Hersteller einen Vertrag über die Überlassung der Daten abschließen könnte.

Für einen solchen Lösungsansatz lässt sich anführen, dass im Strafrecht bereits seit den neunziger Jahren eine Zuordnung von Daten via Skripturakt[28] angenommen wird. Der Schritt zu einem echten „Dateneigentum“ erscheint daher nicht allzu fernliegend. Andererseits ist die Figur des Dateneigentums rechtsdogmatisch problematisch, da Eigentum nur für körperliche Gegenstände definiert ist. Hinzu kommt, dass die Möglichkeit eines Eigentums an Daten dazu führen könnte, dass finanzstarke Akteure große Datenmengen einfach aufkaufen und ausschließlich für ihre eigenen Zwecke verwenden. Es erscheint deshalb im Ergebnis überzeugend, dass die EU sich nicht für die Möglichkeit eines Dateneigentums entschieden hat.

Stattdessen hat sie ein neuartiges Modell entwickelt, welches zwar ein originäres Zugriffs- und Verwendungsrecht der Person anerkennt, durch deren Handeln die Daten entstehen, andererseits aber Maßnahmen vorsieht, um eine Monopolisierung dieser Daten zu verhindern. Der Hersteller eines Produkts wird verpflichtet, den Benutzern des Produkts, also etwa dem Käufer und Fahrer eines Fahrzeugs, den Zugang zu den darin entstandenen Daten zu eröffnen. Dieser hat sodann die Möglichkeit, die Daten selbst zu nutzen, mit anderen zu teilen oder Dritten zur Verfügung zu stellen. Das kann entgeltlich, aber auch unentgeltlich geschehen. Hat der Nutzer kein Interesse an den Daten, so verbleiben sie beim Dateninhaber (Hersteller), der jedoch, wenn er sie verwenden will, eine vertragliche Vereinbarung, einen Datenlizenzvertrag, mit dem Nutzer schließen muss.[29]

Der neue Data Act möchte also einerseits Anreize zur Datenproduktion setzen, andererseits den Zugang zu Daten erleichtern. Für personenbezogene Daten wirft dies Probleme auf, weil diese Daten auch der DSGVO unterfallen. Immerhin wird das Problem von den Verfassern des Data Act durchaus gesehen. In Art. 1 Abs. 3 heißt es:

„Diese Verordnung berührt nicht die Anwendbarkeit der Rechtsvorschriften der Union über den Schutz personenbezogener Daten, insbesondere der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, sowie die Befugnisse und Zuständigkeiten der Aufsichtsbehörden. Soweit die in Kapitel II dieser Verordnung festgelegten Rechte betroffen sind und es sich bei den Nutzern um von der Verarbeitung personenbezogener Daten betroffene Personen handelt, die den Rechten und Pflichten des genannten Kapitels unterliegen, ergänzen die Bestimmungen dieser Verordnung das Recht auf Datenübertragbarkeit nach Artikel 20 der Verordnung (EU) 2016/679".

Doch was soll es bedeuten, dass die Vorgaben der DSVGO durch den Data Act „nicht berührt" werden? Wie ist es gemeint, wenn ausgeführt wird, Art. 20 der DSGVO, der die Übertragung personenbezogener Daten regelt, werde durch das neue Datengesetz „ergänzt"? Um auf unser Pkw-Beispiel zurückzukommen: Im Wagen werden von eingebauten Sensoren Daten über die Nutzung der Bremsen, die gefahrene Strecke, das gefahrene Tempo und den Abrieb der Bremsbeläge aufgenommen und gespeichert. Das sind genau die Informationen, die ein Herstellerunternehmen benötigt. Die Daten lassen sich aber mit hinreichendem Aufwand (z.B. über die Fahrgestellnummer bzw. Fahrzeugidentifikationsnummer) einem Halter zuordnen, über den dann wiederum der Fahrer identifiziert werden kann. Man kann also mit guten Argumenten vertreten, dass es sich um personenbezogene, weil jedenfalls mit leistbarem Aufwand personenbeziehbare Informationen handelt.

Was folgt daraus für die Anwendbarkeit des Data Act einerseits und der DSGVO andererseits? Hier und auch an anderen Stellen kommt es offenbar zu *Regelungskollisionen*, die im Data Act nicht überzeugend aufgelöst werden.

V. Lösungsansätze

Welche Lösungsansätze bieten sich an? Zu denken wäre zuallererst an den Grundsatz, dass das ranghöhere Gesetz dem rangniedrigeren vorgeht. Im Verhältnis von DSGVO und Data Act hilft dieser Grundsatz aber nicht weiter, da auch der Data Act als EU-Verordnung erlassen werden soll, so dass es sich um gleichrangige Regelungsakte handelt.

In Frage kommt weiter der alte Grundsatz, dass das neuere Gesetz das ältere verdrängt (lex posterior derogat legi priori). Dies würde bedeuten, dass die neuen Regelungen des Data Act und der anderen EU-Digitalgesetze damit kollidierende Bestimmungen der DSGVO verdrängen. Gerade angesichts der Ausdeutbarkeit vieler neuer Bestimmungen – viele davon befinden sich allerdings noch im Entwurfsstadium – und der jedenfalls bislang mangelnden wissenschaftlichen Durchdringung des neuen EU-Datenwirtschaftsrechts würde dies allerdings bedeuten, dass die DSGVO in vielfacher und gar nicht näher abgrenzbarer Hinsicht durchlöchert und in ihrer Gesamtwirkung erheblich beeinträchtigt würde. Es spricht nichts dafür, dass der europäische Gesetzgeber Derartiges intendiert hätte.

Unergiebig ist auch eine dritte Möglichkeit zwischen DSGVO und Data Act zu vermitteln, nämlich die Anwendung der Regel, dass das speziellere Gesetz das allgemeinere verdrängt: lex specialis derogat legi generali. Beide Regelungsakte betreffen unterschiedliche Materien, sind also jeweils mit Blick auf den von ihnen geregelten Fragenkomplex „spezieller". Es ist deshalb unklar, welchem Gesetz nach dieser Kollisionsregel der Vorrang gebühren sollte. Ein erster Durchgang durch die klassischen Regeln für eine Normenkollision führt also nicht zu einem befriedigenden Ergebnis.

Im Data Act heißt es, wie eben zitiert, die DSGVO werde durch die neue Regelung „nicht berührt". Wörtlich genommen ist dies unzutreffend oder zumindest wenig aussagekräftig. Man wird die Klausel aber zumindest als Aufforderung an die Rechtswissenschaft und die Rechtsprechung deuten können, eine Harmonisierung zwischen beiden Regelungswerken herzustellen.

Teilweise wird gefordert, angelehnt an den Data Governance Act, dem Datenschutz in allen Kollisionsfällen Vorrang einzuräumen. Eine solcher Ansatz könnte allerdings dazu führen, dass sich das Rechtsregime für den Umgang mit personenbezogenen Daten im Kontext des Datenhandels grundlegend von dem für den Umgang mit nicht personenbezogenen Daten unterscheiden würde, was sich bis hin zur Zuständigkeit der jeweiligen Aufsichtsbehörden auswirken würde. Rein faktisch lassen sich entsprechende Datensätze meist wohl nicht sauber auseinanderhalten, wie das Beispiel mit den Fahrzeugdaten zeigt. Ergebnis wäre ein bürokratisches Monster, das weder dem Bedürfnis nach Datenhandel noch der Notwendigkeit des Datenschutzes gerecht würde.

Hinzu kommt, wie bereits angesprochen, dass die Abgrenzung zwischen personenbezogenen und nicht personenbezogenen Daten unscharf geworden ist und durch die rasante technische Entwicklung immer unschärfer wird. Der potentielle Geltungsbereich der DSGVO erweitert sich damit mehr und mehr, was den Datenschutz nicht verbessert, sondern schwächt, Rechtsunsicherheit schafft und so die bereits heute erheblichen Akzeptanzprobleme verschärft.

Meines Erachtens führt deshalb kein Weg daran vorbei, im Umgang mit unseren Daten einen grundlegenden Neuanfang anzustreben. Angesichts der neuen EU-Vorstöße bedarf das Verhältnis von Datenschutz und Datenhandel einer reflektierten Neujustierung, die bislang noch nicht in ausreichendem Maß geleistet wurde.[30] Das hohe Tempo, mit dem die EU ihre neuen Digitalgesetze vorantreibt, ist deshalb problematisch. Mir erscheint eine Art Moratorium sinnvoll, um die aufgezeigten Spannungen zumindest einmal umfassend zu beschreiben und theoretisch zu erfassen.

Bis dahin sollte der Data Act, ebenso wie der Data Governance Act und die anderen neuen EU-Digitalgesetze, sofern sie schon in Geltung gelangen, im Lichte der DSGVO ausgelegt werden. Wo möglich, sollten auch noch Änderungen im Wortlaut angebracht werden. Ausgangspunkt für eine Harmonisierung von Datenschutz und gemeinwohlorientiertem Datengebrauch muss

der Blick auf die grundrechtlichen Vorgaben des Umgangs mit Daten sein, die durch den Data Act nicht verändert wurden. Sowohl die europäische Grundrechte-Charta (Art. 8) als auch das deutsche Grundgesetz (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1) schreiben den Datenschutz als Grundrecht fest. Aber auch das Eigentum und die unternehmerische Freiheit, ebenso das Interesse an einem wirksamen Gesundheitsschutz, genießen Grundrechtsschutz. Dies legt eine Abwägung im Einzelfall nahe. Sind erst einmal hinreichend viele Fälle diskutiert und gelöst worden, so wird es möglich, Fallgruppen zu bilden und mittels der Kasuistik rechtsstaatliche Regeln zu formulieren.

Nicht ausgeschlossen erscheint auch eine Änderung der DSGVO, um unproblematische und gemeinwohlbezogene Formen des Verfügbarmachens von Daten zu erlauben. Es wird in der Öffentlichkeit nicht immer beachtet, dass die DSGVO bereits heute eine Vielzahl von gut durchdachten Ausnahmetatbeständen enthält, die einen gemeinwohlorientierten Umgang mit Daten möglich machen. Ein Ansatz könnte sein, auf eine Einwilligung oder, in unserem Zusammenhang noch wichtiger, mutmaßliche Einwilligung des Betroffenen abzustellen. Auch die Figur der hypothetischen Einwilligung könnte mutatis mutandis ins Spiel gebracht werden.

Allerdings gibt es Grenzen. Das Recht auf informationelle Selbstbestimmung ergibt sich wie ausgeführt aus Art. 1 Abs. 1 in Verbindung mit Art. 2 Abs. 1 Grundgesetz. Es ist deshalb naheliegend, einen Kernbereich des Rechts auf informationelle Selbstbestimmung sogar direkt in der Menschenwürde, Art. 1 Abs. 1, zu verorten, was bedeuten würde, dass dieser Bereich nicht gesetzlich einschränkbar ist. Ein solcher Kernbereich wäre nach umstrittener, m.E. aber zutreffender Ansicht nicht einmal für den Grundrechtsträger selbst verfügbar, was bedeutet, dass hier Grenzen der Selbstbestimmung erreicht sind. Auch ein konsentierter Handel mit entsprechenden Daten wäre dann ausgeschlossen. Die damit angedeuteten Fragen bedürfen allerdings einer eingehenderen Analyse, als sie hier geleistet werden kann.

VI. Fazit

Damit komme ich zu meinem Fazit: Der Data Act und die anderen EU-Digitalgesetze weisen in die richtige Richtung. Das hohe Tempo, das der EU-Gesetzgeber eingeschlagen hat, führt jedoch dazu, dass die Entwürfe nicht immer hinreichend untereinander und in Bezug auf ältere Regelungen abgestimmt sind. Gerade das Verhältnis des neuen Data Act zur DSGVO wirft viele Fragen auf. Bis sie gelöst sind, ist von einem Vorrang des Datenschutzes auszugehen. Darüber hinaus sollte jedoch über sprachliche Klärungen und Ergänzungen im Entwurf des Data Acts, vielleicht aber auch in der DSGVO nachgedacht werden, um zu helfen, die Vision einer gemeinwohlorientierten Datenwirtschaft bald Wirklichkeit werden zu lassen.

* Bei diesem Text handelt es sich um den Vorabdruck eines im Rahmen des 25. Wiesbadener Forums für Datenschutz am 6. Oktober 2022 anlässlich der Jubiläumsfeier zu „50 Jahre Datenschutz in Hessen" gehaltenen Vortrags. Die Vortragsfassung wurde beibehalten, aber um Anmerkungen ergänzt. Eine ausführlichere Fassung erscheint in: Roßnagel/Wallmann (Hrsg.), Stärkung der Forschung durch Datenschutz, 2023/2024).

1 https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai. Näher dazu Hilgendorf, Gemeinwohlorientierte Gesetzgebung auf Basis der Vorschläge der EU „High Level Expert Group on Artificial Intelligence", in: Piallat (Hrsg.), Der Wert der Digitalisierung. Gemeinwohl in der digitalen Welt, 2021, S. 223-251. Der Verfasser wirkte als einer der deutschen Vertreter in der High Level Expert Group mit.

2 https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en.

3 https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

4 https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

5 https://eur-lex.europa.eu/legal-content/ENTXT/?uri=COM%3A2022%3A68%3AFIN.

6 Dazu eingehend Hilgendorf/Vogel, JZ 2022, S. 380-388.

7 https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age.

8 Richtlinienvorschlag Produkthaftung, COM (2022) 495 final, dazu Wagner, JZ 2023, S. 1 ff.

9 Umfassend Nemitz/Pfeffer, Prinzip Mensch. Macht, Freiheit und Demokratie im Zeitalter der Künstlichen Intelligenz, 2. Aufl. 2020. Paul Nemitz ist Hauptberater in der EU-Kommission, Generaldirektion Justiz und Verbraucherschutz.

10 Siehe oben En. 3, in Kraft getreten am 16.11.2022.

11 Siehe oben En. 3, in Kraft getreten am 01.11.2022.

12 Siehe oben En. 4. Näher Hilgendorf/Roth-Isigkeit, Die neue Verordnung der EU zur Künstlichen Intelligenz: Rechtsfragen und Compliance, 2023. Zum datenschutzrechtlichen Hintergrund Vogel, Künstliche Intelligenz und Datenschutz. Vereinbarkeit intransparenter Systeme mit geltendem Datenschutzrecht und potentielle Regulierungsansätze, 2022.

13 Richtlinienvorschlag KI-Haftung, COM (2022) 496 final, dazu Wagner JZ 2023, S 1 ff.

14 Dazu oben En. 5.

15 Study on Mapping Data flows vom 3.2.2022, https://digital-strategy.ec.europa.eu/en/library/study-mapping-data-flows, wo es heißt: „The final report of the study provides a new and self-sustained methodology to estimate and monitor the volume and types of enterprise data flowing between cloud infrastructures within Europe and for investigating where data is flowing geographically across Europe."

16 Nemitz/Pfeiffer (En. 9), S. 53 ff.

17 Hilgendorf/Vogel, JZ 2022, S. 380.

18 Bradford, The Brussels Effect: How the European Union Rules the World, 2020.

19 Hilgendorf/Kusche/Valerius, Computer- und Internetstrafrecht, 3. Aufl. 2022.

20 BVerfGE 65, 1 ff.

21 Roßnagel, Regulierung – was leistet unser Datenschutzrecht (nicht)?, in: Hill (Hrsg.), e-Transformation, 2014, S. 79 ff. (89).

22 Dazu etwa Hilgendorf, FS für Ulfrid Neumann zum 70. Geburtstag, 2017, S. 1391 ff.

23 Bedrückend realistisch geschildert in Eggers, Every, 2021.

24 Ein Beispiel ist die Debatte um die Klingelschilder und ihre Vereinbarkeit mit der DSGVO, dazu https://www.datenschutz.org/klingelschilder.

25 Hilgendorf, Automatisiertes Fahren und Recht, in: 53. Deutscher Verkehrsgerichtstag. Veröffentlichungen der auf dem 53. Deutschen Verkehrsgerichtstag vom 28.-30. Januar 2015 in Goslar gehaltenen Vorträge, Referate und erarbeiteten Empfehlungen, 2015, S. 55 (65).

26 Zum „Brussels Effect" siehe oben En. 18.

27 Umfassend Haustein, Möglichkeiten und Grenzen von Dateneigentum, 2021.

28 Zu Entwicklung Haustein (En. 27), S. 204 ff.

29 Hennemann/Steinrötter, NJW 2022, S. 1483 sprechen anschaulich von einer „Datenlizenz".

30 Siehe jetzt aber von Lewinski/Rüpke/Eckhardt, Datenschutzrecht. Grundlagen und europarechtliche Neugestaltung, 2022.

Ute Bernhardt/Ingo Ruhmann/Thilo Weichert

EHDS – der Europäische Gesundheitsdatenraum

Das Kürzel EHDS wird Datenschützern künftig öfter begegnen. Es steht für „European Health Data Space". Dabei handelt es sich nicht um einen „Raum" im analogen Sinn, sondern um nichts anderes als eine geplante Verordnung, also ein projektiertes Gesetz der Europäischen Union (EU). Der Entwurf für einen EHDS (EHDS-E)[1] ist Bestandteil der 2020 vorgestellten europäischen Datenstrategie, in der bereichsspezifische Datenräume vorgeschlagen werden.[2] Neben dem für Gesundheit soll es Datenräume u.a. zu Mobilität, Umwelt, Landwirtschaft und Soziales geben (ErwGr 55 S. 8, 11, 12).[3] Mit ihrer Digitalstrategie will die EU-Kommission neben internen Effekten im globalen Wettbewerb einen rechtlichen Rahmen schaffen, mit dem Unternehmen in Europas Digitalwirtschaft insbesondere gegenüber Anbietern aus den USA und China durch rechtsstaatliche und gemeinwohlorientierte Vorgaben Wettbewerbsvorteile geschaffen werden.[4]

Gesetz und informationstechnische Plattform

Der EHDS soll drei Funktionen erfüllen: Zum einen soll er einen rechtlichen und strukturellen Rahmen dafür geben, dass Betroffene, die im Entwurf „natürliche Personen" genannt werden[5], ihre Gesundheitsdaten verwalten können. Außerdem soll der EHDS die Plattform für den grenzüberschreitenden Austausch von Gesundheitsdaten für medizinische Primärzwecke, also insbesondere im Rahmen ärztlicher Behandlung, regeln. Schließlich soll der EHDS die Grundlage für eine Bereitstellung von Gesundheitsdaten für Sekundärzwecke abgeben, insbesondere zur wissenschaftlichen Auswertung für die medizinische Forschung, aber auch für viele weitere Zwecke von der politischen Planung über die medizinische Qualitätssicherung bis hin zu Rückmeldungen in den Behandlungsbereich, etwa im Rahmen personalisierter Therapien.

Der EHDS soll nicht nur mit aggregierten und anonymisierten Daten gefüllt werden, sondern vor allem mit personenbezogenen Gesundheitsdaten, die gemäß Art. 9 Abs. 1 DSGVO als besonders sensitiv und schützenswert eingestuft werden. Damit kann er sich der Aufmerksamkeit der Datenschützer gewiss sein.

Mit dem EHDS sollen die äußerst unterschiedlichen Digitalisierungsniveaus des Gesundheitswesens in den Mitgliedstaaten der EU einander angepasst werden. Ziel ist es in diesem Bereich europaweit die Automation voranzutreiben. Es soll verhindert werden, dass dieser Bereich, der noch weitgehend von EU-Playern bespielt wird, von Unternehmen aus den USA und China übernommen wird. Das ökonomische Potenzial der Gesundheitsdaten wird hoch eingeschätzt. Dieses Potenzial soll gehoben werden, indem ein gemeinsamer Binnenmarkt geschaffen wird. Dieser setzt vor allem gemeinsame Standards und Formate voraus, technische Schnittstellen und Kommunikationsnetze, und letztlich auch ein einheitliches Regelwerk. Der EHDS zielt auf sämtliche dieser Ebenen.

Europäisches Gesundheitsrecht

Bisher spielte das Thema Gesundheit in der EU eine untergeordnete Rolle. Die einzige nennenswerte und informationell relevante Regulierung erfolgte 2011 mit der Patientenrechterichtlinie, mit der Patientenrechte in der grenzüberschreitenden Gesundheitsversorgung fixiert werden.[6] Nach Art. 14 dieser Richtlinie wurde die Plattform MyHealth@EU etabliert, die bisher aber nur in zehn Mitgliedstaaten eingeführt wurde und die nur zwei Dienste (elektronische Verschreibung und Patientenkurzakte) unterstützt. Zudem gibt es EU-Regeln zu Medizinprodukten[7] und zur In-Vitro-Diagnostik.[8] Der Gesundheitsbereich blieb weitgehend eine nationalstaatliche Domäne. Rechtliche Grundlage für Unionspolitiken im Gesundheitsbereich ist Art. 168 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), welcher der EU vorrangig eine ergänzende und fördernde Funktion zu den nationalen Politiken zum Gesundheitsschutz zuweist. Der Gesundheitsschutz hat seit 2009 EU-weit in Art. 35 der europäischen Grundrechte-Charta (GRCh) eine normative Grundlage, der jedem Menschen ein Recht auf Zugang zur Gesundheitsversorgung und auf ärztliche Versorgung zuspricht.

Dass hierfür die nationalen Politiken nicht mehr genügen, wurde den Verantwortlichen in der EU schlagartig mit der Corona-Pandemie klar (ErwGr 2, 3). Dabei ging es nicht nur um die gemeinsame Versorgung mit Impfstoff, sondern auch um möglichst einheitliche Stan-

dards bei der Pandemiebekämpfung, etwa durch einheitliche Impfnachweise[9], und um die möglichst aktuelle und repräsentative Datengewinnung und den Datenaustausch, womit eine bessere Einschätzung der Pandemie ermöglicht würde. Gerade in Deutschland machte die Pandemie schmerzlich bewusst, dass die digitale Rückständigkeit des Gesundheitsbereichs ein Hemmschuh bei der Pandemiebekämpfung war bzw. ist.

Rechtliche Rahmenbedingungen

Der Vorschlag des EHDS steht im Zusammenhang mit zwei weiteren Gesetzesprojekten – dem Data-Governance Act[10] und dem Data Act[11]. Der Data Governance Act benennt allgemeine Bedingungen für die Sekundärnutzung von Daten des öffentlichen Sektors und dient dem Daten-Altruismus ohne ein wirkliches Recht auf Sekundärnutzung solcher Daten zu begründen. Der vorgeschlagene Data Act soll die Übertragbarkeit bestimmter nutzergenerierter Daten verbessern, was Gesundheitsdaten einschließen kann, enthält aber keine Vorschriften für alle Gesundheitsdaten.

Flankierend zum EHDS haben die EU-Gesetzgeber die Verordnung (EU) 2021/522 erlassen, die ein Aktionsprogramm im Bereich der Gesundheit (EU4Health-Programm) für den Zeitraum 2021 bis 2027 einrichtet.[12] Art. 3 lit. c dieser Verordnung nennt die Förderung des Datenaustauschs als Ziel des Aktionsprogramms. Dies wird mit der „Stärkung der Verwendung und Wiederverwendung von Gesundheitsdaten für die Gesundheitsversorgung sowie für Forschung und Innovation, Förderung der Einführung digitaler Instrumente und Dienste sowie des digitalen Wandels der Gesundheitssysteme, indem beispielsweise die Schaffung eines europäischen Raums für Gesundheitsdaten unterstützt wird“, spezifiziert (Art. 4 lit. f EU4Health-Program).

Ihre Gesetzgebungskompetenz für den EHDS leitet die EU aus den Art. 16 (Datenschutz) und Art. 114 (Binnenmarkt) AEUV ab. Damit versteht sich der EHDS als bereichsspezifische Datenschutzgesetzgebung, mit der die DSGVO, die unangetastet bleiben soll (ErwGr 4), konkretisiert wird. Hinsichtlich der Regelungsintensität hat sich die EU-Kommission auf eine mittlere Option festgelegt (EHDS-E S. 16 f.): Die Rechte natürlicher Personen sollen hinsichtlich der digitalen Kontrolle ihrer Gesundheitsdaten gestärkt werden. Die Sekundärnutzung elektronischer Gesundheitsdaten soll sich auf nationale Stellen für die Primär- und Sekundärnutzung elektronischer Gesundheitsdaten stützen. Diese sollen – durch die EU unterstützt – die Maßnahmen auf nationaler Ebene umsetzen. Zwei digitale Infrastrukturen sollen den grenzüberschreitenden Austausch und die Sekundärnutzung elektronischer Gesundheitsdaten ermöglichen. Eine obligatorische Zertifizierung von Electronic-Health-Record(EHR)-Systemen und eine freiwillige Kennzeichnung für Wellness-Apps ist vorgesehen. Ein solches EHR-System, das sich derzeit im Aufbau befindet, ist in Deutschland für gesetzlich Krankenversicherte in den §§ 341 ff. SGB V geregelt.

Es ist erklärtermaßen ein Anliegen des EHDS das in Art. 8 GRCh gewährleistete Grundrecht auf Datenschutz zu stärken (EHDS-E S. 19). Dabei wird umfassend auf die DSGVO Bezug genommen, die in Art. 9 Abs. 1 Gesundheitsdaten besonders schützt und in Art. 9 Abs. 2 neben den Mitgliedstaaten auch der EU die Befugnis zuspricht zur Präzisierung der Verarbeitungsbedingungen bei der Gesundheitsversorgung (lit. h), des öffentlichen Gesundheitswesens (lit. i) und von Forschung, Statistik und Archivwesen (lit. j).

Struktur des EHDS

Der Entwurf des EHDS hat 72 Artikel und ist in 9 Kapitel gegliedert. Kapitel I (Art. 1, 2) legt den Gegenstand und den Anwendungsbereich fest, definiert Begriffe und erläutert die Verknüpfungen mit anderen EU-Instrumenten.

Kapitel II (Art. 3-13) mit der Überschrift „Primärnutzung“ regelt die die DSGVO ergänzenden Rechte für die Betroffenen und Mechanismen für deren Wahrnehmung. Angehörige von Gesundheitsberufen werden zum Führen elektronischer interoperabler Gesundheitsdaten (EHR) verpflichtet. Die Mitgliedstaaten müssen eine digitale Gesundheitsbehörde für die Aufsicht und eine nationale Kontaktstelle für den Datenaustausch einrichten. Der grenzüberschreitende Austausch elektronischer Gesundheitsdaten soll über eine gemeinsame Infrastruktur – MyHealth@EU – abgewickelt werden.

Kapitel III (Art. 14-32) regelt die Selbstzertifizierung der EHR-Systeme und legt Anforderungen in Bezug auf Interoperabilität und Sicherheit fest. Die Pflichten der mit EHR-Systemen befassten Wirtschaftsakteure werden fixiert. Zudem gibt es Bestimmungen über die freiwillige Kennzeichnung von Wellness-Apps, die mit den EHR-Systemen interoperabel sind.

Aus Datenschutzsicht zentral ist Kapitel IV (Art. 33-58) zur Sekundärnutzung elektronischer Gesundheitsdaten, z.B. für Forschung, Innovation, Politikgestaltung, Patientensicherheit oder Regulierungstätigkeiten. Darin werden Datenarten benannt, die für die Sekundärzwecke verwendet werden können, und es werden unzulässige Zwecke festgelegt (z.B. Nutzung von Daten zum Schaden von Personen, kommerzielle Werbung, Erhöhung der Versicherung, Entwicklung gefährlicher Produkte). Die Mitgliedstaaten richten Stellen für den Datenzugang zwecks Sekundärnutzung ein. Die Rahmenbedingungen des Datenaltruismus im Gesundheitswesen und die Zuständigkeiten und Pflichten der Stellen für den Zugang zu Gesundheitsdaten und der Datennutzer werden festgelegt.

Kapitel V (Art. 59-63) regelt strukturelle Rahmenbedingungen, u.a. zum Austausch von Informationen über digitale öffentliche Dienste, Finanzierung usw. sowie zum internationalen Zugang zu nicht personenbezogenen Daten im EHDS. Kapitel VI (Art. 64-66) führt einen Ausschuss für den europäischen Raum für Gesundheitsdaten (European Health Data Space Board, EHDS-Ausschuss) ein, der die nationalen digitalen Gesundheitsbehörden und die Stellen für den Zugang zu Gesundheitsdaten koordiniert. Zudem gibt es Bestimmungen zur gemeinsamen Verantwortlichkeit in der EU-Infrastruktur. Kapitel VII (Art. 67, 68) gibt der EU-Kommission weit gehende Befugnisse zum Erlass von delegierten Rechtsakten; Kapitel VIII (Art. 69-71) sieht nationale Sanktionen bei Verstößen gegen den EHDS und eine Evaluierung des EHDS vor. Kapitel IX (Art. 72) enthält Schlussbestimmungen.

Betroffenenrechte und geplante IT-Struktur

In Ergänzung zu Art. 15 DSGVO verspricht Art. 3 EHDS-E Betroffenen einen elektronischen Zugriff auf Primärnutzungsdaten „sofort, kostenlos und in einem leicht lesbaren, gängigen und zugänglichen Format" sowie ein Recht auf eine „elektronische Kopie". Diese Rechte können durch nationale Regelung aus Gründen der Patientensicherheit und aus ethischen Gründen beschränkt werden, so wie dies z.B. in § 630g Abs. 1 BGB („therapeutische Gründe") schon gilt. Der Zugriff auf die Daten im Rahmen der Primärnutzung, also zwecks Behandlung im weitesten Sinne (Art. 2 Abs. 2 lit. d), kann durch die Betroffenen Gesundheitsberufen ganz oder teilweise beschränkt werden (Art. 3 Abs. 9).[13]

Die Mitgliedstaaten werden verpflichtet, digitale Zugangsdienste einzurichten, mit denen die Betroffenen auf die eigenen Gesundheitsdaten und die elektronische Patientenakte zugreifen können, einschließlich der Möglichkeiten zur eigenen Dateneingabe, zur Wahrnehmung der allgemeinen Betroffenenrechte sowie zur Freischaltung für andere Gesundheitsdienstleister (Art. 4). Patientenkurzakten, elektronische Verschreibungen, elektronische Abgaben, medizinische Bilder und Bildbefunde und Entlassungsberichte sollen vorrangig digital bereitgestellt werden (Art. 5 Abs. 1, Anhang I). Diese Datenkategorien müssen gemäß nationaler Regelungen von den Gesundheitsberufen in der EHR (Electronic Health Record – elektronischen Patientenakte) angeliefert werden (Art. 7). Die Authentifizierung aller Beteiligten wird über ein digitales Identifizierungsmanagement (Art. 9) sichergestellt. Betroffene können sich, wenn ihre Rechte eingeschränkt scheinen, bei der digitalen Gesundheitsbehörde beschweren, die mit der zuständigen Datenschutzbehörde zusammenarbeitet (Art. 11).

Als grenzüberschreitende Infrastruktur wird von der EU die zentrale Plattform „MyHealth@EU" eingerichtet, die über eine nationale Kontaktstelle in jedem Mitgliedstaat erreichbar gemacht wird, welche wiederum elektronisch mit den nationalen Gesundheitsdienstleistern verknüpft wird (Art. 12). Über MyHealth@EU können auch weitere Gesundheitsdienste, z.B. der Telemedizin verknüpft werden (Art. 13). In die dezentral geführten EHR-Systeme können in strukturierter Weise auch Daten von Medizinprodukten, also u.a. die Digitalen Gesundheitsanwendungen (DiGa, vgl. § 33c SGB V) sowie Wellness-Anwendungen eingebunden werden (Art. 14-31).

Datenbereitstellung zur Sekundärnutzung

Art. 33 sieht vor, dass Dateninhaber für Sekundärnutzungen viele verschiedene Kategorien von Gesundheitsdaten über die Zugangsstelle (Art. 41 Abs. 1) zur Verfügung stellen müssen. Die Verpflichtung zur Bereitstellung und Übermittlung dieser Daten ist eine rechtliche Pflicht i.S.v. Art. 6 Abs. 1 lit. c DSGVO (ErwGr 37 S. 4). Der Begriff „Dateninhaber", der private wie öffentliche Stellen einschließt (ErwGr 40 S. 1), ist dem Datenschutzrecht bisher unbekannt. Dies sind gemäß Art. 2 Abs. 2 lit. y Einrichtungen im Gesundheitsbereich im weiten Sinne, die „durch Kontrolle eines technischen Produkts und der damit zusammenhängenden Dienste dazu befähigt sind bestimmte Daten zur Verfügung zu stellen". Weshalb hier nicht auf die etablierte Figur des „Verantwortlichen" zurückgegriffen wurde, ist nicht eindeutig ersichtlich; unklar ist, ob damit auch Auftragsverarbeiter (Art. 4 Nr. 8, 28 DSGVO) einbezogen werden sollen;[14] die Definition bezieht auch Stellen mit ein, deren Gesundheitsdaten nicht personenbezogen sind. Nicht verpflichtet werden Kleinstunternehmen.

Die von der Pflicht erfassten Datenkategorien sind denkbar weit: elektronische Patientenakten, gesundheitsrelevante (soziale, umweltbedingte, verhaltensbezogene) Faktoren, genetische und proteomische Daten, Verwaltungsdaten, Daten aus digitalen Anwendungen von Medizin- bis zu Wellness-Produkten, Daten aus Registern, Biobanken und sonstigen Datenbanken, aus klinischen Prüfungen, aus der Forschung sowie daraus generierte oder veränderte Daten (Art. 3 Abs. 1). Man kann den Eindruck haben, dass alle Daten, die auch im entferntesten einen Gesundheitsbezug haben, von der Bereitstellungspflicht erfasst sein sollen.

Zugang zu diesen Daten wird gewährt, wenn einer der folgenden Zwecke verfolgt wird: Tätigkeiten im Bereich der öffentlichen Gesundheit und im öffentlichen Interesse, Statistik, Bildungs- und Lehrtätigkeit, Forschung, Entwicklung und Innovation von Produkten und Diensten, Training und Bewertung von Algorithmen und personalisierte Gesundheitsversorgung (Art. 34 Abs. 1, ErwGr 41). Mit diesen Zwecken sollen die in den Art. 9 Abs. 2 lit. h, i u. j DSGVO definierten Ausnahmen vom Verarbeitungsverbot sensitiver Daten abgedeckt werden (ErwGr 37 S. 5). Offensichtlich wegen der Breite der möglichen Zwecke wird auch ein Ausschlusskatalog aufgeführt: Das Treffen von für Menschen schädlichen Entscheidungen, Werbung, Marketing, Entwicklung von Drogen und ähnlichen Produkten und die Weitergabe an nicht autorisierte Stellen soll im Rahmen der Sekundärnutzung nicht erlaubt sein (Art. 35).

Als Rechtsgrundlage der Datennutzenden kommt gemäß den Entwurfsverfassern sowohl ein öffentliches Interesse i.S.v. Art. 6 Abs. 1 1 lit. e DSGVO in Betracht, was eine Konkretisierung durch weitere Rechtsvorschriften voraussetzt (ErwGr 37 S. 9), als auch ein überwiegendes berechtigtes Interesse i.S.v. Art. 6 Abs. 1 lit. f DSGVO. In diesen Fällen soll der EHDS selbst als Rechtsgrundlage genügen. Die einzuhaltenden Garantien müssten, so die Kommission, über die Datengenehmigung „in den Bedingungen für den Datenzugang festgelegt werden" (ErwGr 37 S. 10, 11).

Zugangsstellen

Der Datenzugang erfolgt über eine oder mehrere weisungsfreie „Zugangsstellen", die von den Mitgliedstaaten eingerichtet werden. Sie erfüllen eine Funktion des öffentlichen Interesses i.S.v. Art. 6 Abs. 1 lit. e DSGVO (ErwGr 37 S. 6). Sie müssen personell, technisch und finanziell adäquat ausgestattet sein und sollen mit „Vertretern von Patienten, Dateninhabern und Datennutzern" zusammenarbeiten, wobei Interessenkonflikte zu vermeiden sind (Art. 36). Die nach nationalem Recht

zu benennenden Zugangsstellen können sich nach Organisation und Größe unterscheiden, sollen aber „dieselben Funktionen, Zuständigkeiten und Fähigkeiten" haben (ErwGr 42 S. 6).

Die Zugangsstellen entscheiden über die Anträge auf Datenzugang und stellen eine umfassende Infrastruktur zur Entgegennahme, Aufbereitung und Bereitstellung der Gesundheitsdaten für Sekundärzwecke bereit (Art. 37, ErwGr 43). Ihnen kommen allgemeine Informationspflichten gegenüber der Öffentlichkeit zu (Art. 38); sie veröffentlichen zudem jährliche spezifische Berichte über die konkreten Zugangsaktivitäten (Art. 39).

Damit die Zugangsstellen die Datenvermittlung durchführen können haben die Dateninhaber ihre Datenbestände präzise zu beschreiben. Wird ein Antrag von der Zugangsstelle positiv beschieden, müssen die Daten von den Dateninhabern innerhalb von zwei Monaten zur Verfügung gestellt werden. Die Zugangsgewährung ist grds. gebührenpflichtig, wobei sowohl die Aufwände der Zugangsstelle als auch des Datenhalters ersetzt werden können (Art. 42). Verstöße gegen den EHDS durch den Datennutzer wie durch den Dateninhaber können von der Zugangsstelle gemäß nationalem Recht sanktioniert werden (Art. 43, 69, ErwGr 48). Handelt es sich um nicht-personenbezogene Daten, so wird der Zugang „mithilfe vertrauenswürdiger offener Datenbanken" ermöglicht (Art. 41).

Datenzugangsgenehmigung

Aus Datenschutzsicht relevant sind die Regeln zur Datenzugangsgenehmigung. Nach nationalem Recht kann zusätzlich eine Ethikprüfung vorgesehen sein (ErwGr 46 S. 2, 50 S. 5). Die Daten dürfen nur für den genehmigten Zweck genutzt werden und vom Umfang nicht über das hierfür Erforderliche hinausgehen, wenn nicht schon anonymisierte Daten hierfür genügen (Art. 44). Das Gebot der Datenminimierung (Art. 5 Abs. 1 lit. c DSGVO) wird also bestätigt. Es kann demnach gerechtfertigt sein, pseudonyme oder gar identifizierende Daten herauszuverlangen und zu erhalten. Eine entsprechende Regelung (ohne Herausgabe von identifizierenden Daten) ist derzeit in Deutschland durch § 303e SGB V für die Zugangsmöglichkeit zu Daten im Forschungsdatenzentrum des Bundesinstituts für Arzneimittel und Medizinprodukte (BfArM) vorgesehen. Dieses Forschungsdatenzentrum wurde durch das Digitale-Versorgung-Gesetz (DVG) von 2019 eingerichtet.[15]

Antragsberechtigt ist jede natürliche oder juristische Person. Der Antrag muss detaillierte Angaben enthalten zur beabsichtigten Verwendung und Nutzungsdauer, zu den benötigten Daten, zu Vorkehrungen zur Sicherung der technisch und organisatorisch gewährleisteten Vertraulichkeit sowie der Betroffenenrechte (Art. 45 Abs. 2). Eine Datenbereitstellung kann auch europaweit beantragt werden, die dann über eine grenzüberschreitende Infrastruktur (HealthData@EU) erfolgt (Art. 45 Abs. 3, 52).

Die Zugangsstelle prüft den Antrag und genehmigt diesen, evtl. partiell oder unter Bedingungen, bzw. lehnt diesen ab. Im Fall der Genehmigung werden die Daten beim Dateninhaber von der Zugangsstelle angefordert, beschafft und dem Datennutzer bereitgestellt. Werden für eine Anfrage nur Daten eines Dateninhabers angefordert, so ist ein vereinfachtes Verfahren möglich (Art. 49, ErwGr 53). Um den Dateninhabern einen Anreiz zu schaffen ihre Daten zur Verfügung zu stellen, sollen die Datennutzenden, nach „Anreicherung" der im Rahmen der Datennutzung erlangten neuen Daten, diese dem ursprünglichen Dateninhaber zur Verfügung stellen, „um die Verbesserung der ursprünglichen Datenbank und die anschließende Nutzung der angereicherten Datensätze zu unterstützen" (ErwGr 39 S. 4).

Datenbereitstellung und -nutzung

Der Datenzugang wird über eine von der Zugangsstelle geschaffene „sichere Verarbeitungsumgebung" gewährt (Art. 50, ErwGr 54). Datennutzer und Zugangsstelle gelten im Sinne des Datenschutzrechts als „gemeinsam Verantwortliche" (Art. 51). Die Datennutzung ist pro Genehmigung für maximal 5 Jahre möglich. Ergeben sich aus der Datennutzung „klinisch signifikante Befunde", so müssen diese der Zugangsstelle mitgeteilt werden (Art. 46 Abs. 12). Nach Abschluss der Datennutzung muss der Datennutzer einen Bericht über die Nutzung und die dabei erlangten Ergebnisse abliefern, die in den Jahresbericht und in die Webseitenveröffentlichung der Zugangsstelle einfließen (Art. 46 Abs. 11). Über eine „Datenanfrage" kann jeder und jede bei der Zugangsstelle eine Beschreibung des erwarteten Resultats einfordern (Art. 47).

Für grenzüberschreitende Register gibt es eine Sonderregelung (Art. 53). Bei grenzüberschreitenden Projekten bleibt es bei den nationalen Zuständigkeiten bzgl. des Datenzugangs, wobei aber eine Genehmigung von anderen Zugangsstellen anerkannt werden kann (Art. 54, ErwGr 57). Möglich ist auch eine – vorrangig anonyme – Übertragung in Drittländer, sogar unter engen Voraussetzungen, wenn „das Risiko einer Rekonstruktion der Identität" der Betroffenen besteht (Art. 61-64). Die Zugangsstellen geben Informationen über die verfügbaren, evtl. qualitätsgesicherten (Art. 56) Datensätze, damit die potenziellen Datennutzer deren Nutzen einschätzen können (Art. 53).

Organisatorisches

Auf nationaler Ebene ist eine digitale Gesundheitsbehörde einzurichten, die für die Durchsetzung des EHDS zuständig ist (Art. 10). Diese nationalen Gesundheitsbehörden arbeiten zusammen und haben auch mit anderen tangierten Aufsichtsbehörden zu kooperieren. Dies gilt auch für die unabhängigen Datenschutzbehörden, denen die Gesundheitsbehörden Beschwerden, die den Datenschutz betreffen, mitteilen (Art. 10 Abs. 2 lit. n, 11 Abs. 1).[16]

Es wird auf EU-Ebene ein von der EU-Kommission geleiteter EHDS-Ausschuss eingerichtet, der eine Koordinierungsfunktion erfüllen soll. Dort sitzen „hochrangige Vertreter der digitalen Gesundheitsbehörden und der Zugangsstellen". Dieser Ausschuss soll mit den Marktüberwachungsbehörden, dem Europäischen Datenschutzausschuss (EDSA) sowie dem Europäischen Datenschutzbeauftragten (EDPS) sowie mit „Interessenträgern" kooperieren (Art. 64, 65, ErwGr 65).

Von der Kommission eingerichtet werden zudem zwei „Gruppen der gemein-

sam Verantwortlichen für Infrastrukturen", die für die Entwicklung und den Betrieb der grenzüberschreitenden Infrastrukturen und die Interoperabilität verantwortlich zeichnen (Art. 66).

Der EHDS-Vorschlag der EU-Kommission überträgt diesem europäischen Exekutivgremium eine große Machtfülle durch die Befugnis delegierte Rechtsakte zu praktisch allen wesentlichen Fragen zu erlassen. Dem Europäischen Parlament (EP) und dem Europäischen Rat wird hinsichtlich der Rechtsakte ein Vetorecht zugestanden (Art. 67). Es ist auch die Kommission, die nach 5 bzw. nach 7 Jahren eine Evaluation des EHDS vornimmt (Art. 70).

Grundsätzliche Erwägungen

Der Ansatz, bei der Verarbeitung von Gesundheitsdaten eine Vereinheitlichung in Europa anzustreben, ist zu begrüßen. Die EU ist nicht nur ein Binnenmarkt mit Freizügigkeit, sondern auch eine Wertegemeinschaft und ein Gebiet gemeinsamer Lebensbedingungen, die es gemeinsam zu gestalten gilt.

Die Wertegemeinschaft findet ihre Ausgestaltung in der europäischen Grundrechte-Charta, in der individuelle und kollektive Grundprinzipien unserer Gesellschaftsordnung festgehalten sind. Hierzu gehören u.a. mit einem Gesundheitsbezug die Würdegarantie (Art. 1 GRCh), das Recht auf Unversehrtheit (Art. 3 GRCh), die Achtung des Privat- und Familienlebens (Art. 7 GRCh), der Datenschutz (Art. 8 GRCh), die Freiheit der Wissenschaft (Art. 13 GRCh), die Berufsfreiheit und die Unternehmensfreiheit (Art. 16, 17) und der Schutz vor Diskriminierung (Art. 21 GRCh). Besondere Kollektive bedürfen eines spezifischen Schutzes, so Kinder (Art. 24, 32 S. 3 GRCh), ältere Menschen (Art. 25 GRCh) und Menschen mit Behinderung (Art. 26). Dem Gesundheitsschutz wird eine wichtige Bedeutung beigemessen (Art. 35 GRCh) – auch milieubezogen in Bezug auf die Arbeit (Art. 31 Abs. 1 GRCh), die Umwelt (Art. 37 GRCh) sowie für den Bereich des Konsums (Verbraucherschutz, Art. 38 GRCh).

Innerhalb der EU bestehen – wegen unterschiedlicher Traditionen aber auch wegen des bisher geltenden Primats nationaler Regulierung – äußerst unterschiedliche Gesundheitssysteme. Diese Unterschiede in der Gesundheitsversorgung bei Regulierung, Organisation, Finanzierung und technischer und personeller Ausstattung erschweren den Austausch und die Koordination und Kooperation. Es ist nachvollziehbar und gut begründet, wenn die EU dies ändern will. Das Argument der Subsidiarität von EU-Zuständigkeiten (Art. 5 EUV) greift daher nicht zur Verhinderung der vorgesehenen verstärkten Harmonisierung und Kooperation (ErwGr 67). Dies gilt seit den Erfahrungen mit der Corona-Pandemie. Hierbei zeigte sich, dass Gesundheitsrisiken an Staatsgrenzen keinen Halt machen und ein EU-weites gemeinsames Vorgehen oft unabdingbar ist.

Für dieses gemeinsame Vorgehen ist ein koordinierter und gemeinsamer Umgang mit Gesundheitsdaten in vielen Fallgestaltungen zwingend. Es ist insofern nicht zu beanstanden, dass die EU ihre Zuständigkeit für Datenschutz und für den Binnenmarkt (Art. 16, 114 AEUV) nutzt, um eine Spezifizierung der DSGVO hinsichtlich Gesundheitsdaten vorzunehmen, auch wenn dabei die Ziele des (gemeinsamen) Gesundheitsschutzes im Vordergrund stehen. Datenschutz und grenzüberschreitender freier Datenfluss sind zentrale Aspekte für diesen Gesundheitsschutz.

Paradigmenwechsel

Der EHDS bricht mit einem uralten Grundsatz bei der Verarbeitung mit Gesundheitsdaten, wonach das Patientengeheimnis bzw. die ärztliche Schweigepflicht, also die Wahrung der Vertraulichkeit im Verhältnis zwischen Hilfsbedürftigen und Helfenden, oberste Priorität hat. Diese Priorität, von der noch heute das deutsche Gesundheitsdatenrecht geprägt ist, wird aber nicht erstmals durch den EHDS in Frage gestellt. So spricht die DSGVO hinsichtlich der Verarbeitung sensitiver Daten – und damit von Gesundheitsdaten – den Zwecken der Forschung, der Statistik und des Archivwesens einen gleichen Rang zu (Art. 5 Abs. 1 lit. b DSGVO).[17] Der EHDS geht einen Schritt weiter, indem er sich nicht allein auf diese Zwecke beschränkt, sondern den kollektiven Gesundheitsschutz generell als gleichrangig neben dem individuellen Gesundheitsschutz anerkennt. Dabei bleibt er dem in der DSGVO vorgegebenen Anliegen treu praktische Konkordanz bzw. eine Zieloptimierung zu erreichen, was durch spezifische „Bedingungen und Garantien" erfolgen soll.

Der EHDS setzt die Idee der Sozialpflichtigkeit von Gesundheitsdaten um. Diese Pflichtigkeit setzt ein vorrangiges öffentliches Interesse voraus. Auch insofern steht der EHDS in der Tradition der DSGVO.[18] Während aber bisher die Sozialpflichtigkeit der Gesundheitsdaten lediglich ein Aspekt für den Umgang im Einzelfall war, wird mit dem EHDS ein struktureller Rechtsrahmen für praktisch alle Gesundheitsdaten geschaffen. Der damit verbundene Paradigmenwechsel ist noch nicht in der öffentlichen Wahrnehmung und im gesellschaftlichen Bewusstsein angekommen. Er wird auch nicht als solcher klar benannt und diskutiert. Es gibt aber genügend Hinweise dafür, dass dieser Wechsel angesichts der Entwicklungen von Technik, Gesellschaft und Gesundheitswesen geboten ist. So plädierte die Datenethikkommission für harmonisierte abwägende Regelungen zur Forschungsnutzung von Gesundheitsdaten.[19] Der Sachverständigenrat der Bundesregierung zur Begutachtung der Entwicklung im Gesundheitswesen schlug 2021 ein bereichsspezifisches Gesundheitsdatennutzungsgesetz vor.[20] Und tatsächlich findet sich im Koalitionsvertrag der rot-grün-gelben Bundesregierung von 2021 die Ankündigung ein Forschungsdatengesetz zu erlassen, eine nationale Forschungsdateninfrastruktur und einen Europäischen Forschungsdatenraum voranzutreiben und ein Gesundheitsdatennutzungsgesetz auf den Weg zu bringen.[21]

Datenschutz contra Sozialpflichtigkeit

Es war und ist bisher offen, wie die Vorgaben der Grundrechtecharta zum Datenschutz und zur Forschungsfreiheit sowie zu weiteren Grundrechten regulativ zusammengebracht werden können. So ist es nicht verwunderlich, dass Datenschützer umgehend ihren Widerstand gegen den EHDS erklärt haben. In einer Stellungnahme der Initia-

tive „Patientenrechte und Datenschutz“ wird der EHDS als „Ermächtigungsgesetz“ bezeichnet. Zum Schutz des Arzt-Patientenverhältnisses bedürfe es bei der Weitergabe von Daten an Dritte der „Zustimmung der Betroffenen in jedem Einzelfall“. Der EHDS dürfe nicht zum Einfallstor für den Datenhandel mit Patientenakten werden. Zudem seien die technischen Schutzregeln unzureichend. Selbst eine Auslagerung der Verarbeitung an US-Cloud-Anbieter sei beim EHDS-E nicht ausgeschlossen. Schließlich wird geltend gemacht, dass die EU keine Regelungsbefugnis habe, da „die Verwaltung des Gesundheitswesens und der medizinischen Versorgung“ im alleinigen Zuständigkeitsbereich der Mitgliedstaaten liege.[22]

Diese ernst zu nehmenden Bedenken legen ihre Finger in offene Wunden. Sie können und dürfen aber nicht die letzten Antworten des Datenschutzes zum EHDS sein. Sie sind auch nicht geeignet den Datenschutz im Gesundheitswesen mittelfristig zu sichern, da sie die Möglichkeiten und Notwendigkeiten von Sekundärnutzungen der Gesundheitsdaten ignorieren. Es sollte unstreitig sein, dass es einen Ausgleich zwischen Datenschutz und öffentlichen Interessen an der Auswertung von Gesundheitsdaten geben muss und dass insofern bei der Sekundärnutzung den individuellen Datenschutzrechten der Betroffenen nicht generell der Vorrang eingeräumt werden kann.

Hinsichtlich der Kompetenzzuweisung an die EU erscheint der Rückgriff auf die Zuständigkeit für Datenschutz und Binnenmarkt ausreichend (Art. 16, 114 AEUV). Eine Verletzung des Subsidiaritätsgrundsatzes kann angesichts der dringenden Notwendigkeit der informationellen Kooperation im Gesundheitsbereich nicht festgestellt werden. Dessen ungeachtet erscheint die bisherige Regelung des Art. 168 AEUV angesichts der bei der Corona-Pandemie gemachten Erfahrungen nicht mehr zeitgemäß und deshalb entwicklungsbedürftig.

Der EHDS knüpft mit seinen Mechanismen an die Entwürfe für einen Data Act und einen Data Governance Act an, die ein allgemeines Datenregime vorsehen; er unterscheidet sich strukturell hiervon nur in Einzelaspekten. Dabei gerät aus dem Blick, dass es sich bei den im EHDS verarbeiteten Daten um sensitive Daten i.S.v. Art. 9 DSGVO handelt, ja regelmäßig um besonders schützenswerte sensitive Daten. Psychiatrische oder genetische Daten[23] haben einen starken Würdebezug; ihre Aussagekraft berührt den Kernbereich privater Lebensgestaltung. Gesundheitsdaten werden von den Betroffenen oft als existenziell wahrgenommen und sie sind dies in sehr vielen Fällen. Das Regelwerk des EHDS-E nimmt insofern nicht die zwingend nötigen normativen Differenzierungen vor.

Abwägungsdefizite

Hinsichtlich der Betroffenenrechte bei der Sekundärnutzung ist der EHDS restriktiv und in vieler Hinsicht unklar. Gemäß Art. 38 Abs. 1 u. 2 erfolgt eine allgemeine Information über die Tätigkeit der Zugangsstellen. Hierdurch sollen sie von der Unterrichtungspflicht nach Art. 14 DSGVO befreit sein. Diese Ausnahme folgt dem in der DSGVO angelegten Prinzip, dass die individuelle Benachrichtigung durch eine gesetzliche Regelung ersetzt werden kann (Art. 14 Abs. 5 lit. c DSGVO).[24]

Zu den weiteren datenschutzrechtlichen Betroffenenrechten schweigt sich der EHDS-E aus. Damit folgt der EHDS-E dem Regelungskonzept des deutschen Forschungsdatenzentrums.[25] Angesichts des Umstands, dass zu Art. 14 DSGVO eine Ausnahmeregelung besteht, nicht aber zu den anderen Betroffenenrechten in der DSGVO, sollte man davon ausgehen, dass diese Rechte auch bzgl. der Sekundärdatennutzung gelten sollen. Evident ist dies jedoch nicht, zumal die Betroffenendaten hier regelmäßig pseudonymisiert sein werden und dann die Umsetzung der Betroffenenrechte erschwert oder gar ausgeschlossen sein können (vgl. Art. 11 DSGVO). Der Ausschluss des Widerspruchsrechts gemäß Art. 21 Abs. 1 DSGVO bzgl. der Erfüllung einer rechtlichen Pflicht (Art. 6 Abs. 1 lit. c DSGVO)[26] bezieht sich allenfalls auf die Bereitstellungspflicht gegenüber den Zugangsstellen, erfasst aber nicht deren Weitergabe an die Datenempfänger, die auf Art. 6 Abs. 1 lit. e oder lit. f DSGVO basiert. Hier bedarf es nicht nur der Klarstellung, sondern darüber hinausgehend auch spezifischer Mechanismen, mit denen insbesondere das Auskunfts- und das Widerspruchsrecht[27] durch eine organisierte Rückführung des Pseudonyms zu Identitätsdaten bei pseudonymer Verarbeitung gewährleistet werden kann.

Nicht akzeptabel ist der Ansatz des EHDS-E für die Sekundärnutzung als Rechtsgrundlage Art. 6 Abs. 1 lit. f DSGVO, also die Geltendmachung eines berechtigten Interesses, zuzulassen. Dies gilt für jedes private berechtigte Interesse, auch wenn dies nicht durch ein öffentliches Interesse unterstützt wird.[28] Selbst wenn die Anwendung dieser Regelung materiell durch Art. 9 Abs. 2 lit. h, i u. j DSGVO eingeschränkt interpretiert wird, kann dies nicht dem Grundrechtsschutz und auch nicht den Anforderungen der DSGVO genügen. Die DSGVO fordert spezifizierte Garantien und Maßnahmen, die im EHDS-E, entgegen eigenen Beteuerungen (so z.B. S. 19), nicht hinreichend vorgesehen sind.[29] Auch insofern verblüfft und erschreckt das aktuelle Konzept des EHDS hinsichtlich seiner Ähnlichkeit mit den offensichtlich verfassungswidrigen Regelungen zum deutschen Forschungsdatenzentrum.[30]

Ungenügende Bestimmtheit

Eine verfassungsrechtlich relevante Ähnlichkeit zwischen der Datentransparenz gemäß §§ 303a ff. SGB V und dem EHDS-E besteht auch hinsichtlich der Zwecke. In der öffentlichen Darstellung wird zur Rechtfertigung des EHDS regelmäßig auf dessen Notwendigkeit für die medizinische Forschung und den damit möglichen Fortschritt im Gesundheitsbereich hingewiesen. Der EHDS verfolgt bzgl. der Sekundärnutzung aber ein viel breiteres Zweckspektrum. So sieht Art. 34 Abs. 1 vor, dass die Daten genutzt werden können zur Unterstützung jeglicher Art von Stellen „im Gesundheits- und Pflegesektor bei der Wahrnehmung ihrer in ihren Mandaten festgelegten Aufgaben“ (lit. b), für „Bildungs- und Lehrtätigkeiten im Gesundheits- und Pflegesektor“ (lit. d), für jegliche „Entwicklungs- und Innovationstätigkeiten für Produkte und Dienste“ im Gesundheitsbereich (lit. f) oder zu „Training, Erprobung und Bewertung von Algorithmen“ mit Medizinbezug (lit.g). Die

Regelung verzichtet gar auf Einschränkungen hinsichtlich einer, evtl. gesteigerten, Erforderlichkeit und begnügt sich „Relevanz" zu verlangen (Art. 44 Abs. 1). Um verhältnismäßig zu sein müssen die Verwendungszwecke reduziert werden auf solche, mit denen prospektiv ein erheblicher Gewinn für die öffentliche Gesundheit einhergeht.[31] Dies schließt einen individuellen Gesundheitsgewinn nicht aus, da das Wohl eines Einzelnen auch im öffentlichen Interesse liegt.

Angesichts der Offenheit und Breite der zugelassenen Zwecke kommt es für die Bereitstellung in jedem Fall auf eine Abwägung an, für die im EHDS-E nur wenige Anhaltspunkte bereitgestellt werden. Selbst wenn man die in Art. 9 Abs. 2 lit. h, i und j DSGVO aufgeführten Zwecke mitliest, was sich nicht direkt aufdrängt, bleibt man hinsichtlich der Abwägung bei der Genehmigung der Zugangsberechtigung im Ungewissen. Wenig hilfreich ist dabei, dass viele Zwecke keinen oder zumindest nur einen sehr indirekten Grundrechtsbezug haben.

Wo bleibt die Forschungsprivilegierung?

Dies gilt nicht für die medizinische Forschung (Art. 34 Abs. 1 lit. e), die in Art. 13 S. 1 GRCh garantiert ist. Dies gilt auch nicht hinsichtlich der „Bereitstellung einer personalisierten Gesundheitsversorgung" für eine konkrete natürliche Person (lit. h), wo der individuelle Gesundheitsschutz im Spiel ist (Art. 3 GRCh). Trotz der verfassungsrechtlich äußerst unterschiedlich zu bewertenden Zwecke werden sie im EHDS materiell- wie prozessrechtlich völlig gleichbehandelt. Damit wird gegen den Grundsatz verstoßen, dass wesentlich Unterschiedliches auch unterschiedlich zu behandeln ist.

Die Einheitsregelung zum Datenzugang findet auch in der DSGVO keine Grundlage. Die DSGVO privilegiert ausschließlich Statistik, Forschung und Archivwesen in Bezug auf die Zweckänderung (Art. 5 Abs. 1 lit. b DSGVO) und die Betroffenenrechte. Sie erlaubt keine pauschale Vorgehensweise. Für die privilegierten Zwecke wird lediglich eine Flexibilisierung des Datenschutzes eröffnet.[32] Gemäß Art. 89 Abs. 1 DSGVO sind für die Vorzugsbehandlung der Forschungsnutzung in jedem konkreten Einzelfall geeignete Garantien zu geben, von denen aber im EHDS allenfalls allgemein die Rede ist. Selbst bei den privilegierten Forschungszwecken gilt, dass der zulässige Umfang und die Verarbeitungstiefe und Auswertungsintensität sensitiver Daten immer von dem Niveau des Schutzes durch geeignete Garantien und Maßnahmen abhängt.[33]

Eine Privilegierung der Forschung gegenüber den sonstigen in Art. 34 Abs. 1 genannten Zwecken setzt zudem voraus, dass der Begriff der Forschung geklärt ist. Dies ist aber weder beim Forschungsdatenzentrum der Fall[34] noch beim EHDS-E. Es hätte nahegelegen die einschränkende Definition des Bundesverfassungsgerichts zu übernehmen, für die es bisher keine allgemeine gesetzliche Umsetzung gibt und die europarechtlich bisher nicht anerkannt ist.[35]

Unabhängige Zugangsstellen

Ein weiteres Regelungsdefizit bei der Datennutzung durch wissenschaftliche Forschung in den §§ 303a SGB V findet sich auch im EHDS-E: Forschung muss, um Grundrechtseingriffe bei Dritten rechtfertigen zu können, unabhängig sein.[36] Sollen die Grundrechtseingriffe, wie beim EHDS, über die Zugangsstellen und die Datenhalter, also über Dritte vermittelt werden, so muss auch der Prozess des Grundrechtseingriffs gewährleisten, dass dies im Interesse unabhängiger Forschung erfolgt. Dies wird im EHDS-E nicht gewährleistet. Der EHDS-E überlässt es den Mitgliedstaaten weitgehend, wie sie die Zugangsstellen organisieren. Diese werden zur Zusammenarbeit mit Vertretern der Interessenträger angehalten, namentlich der Patienten, Dateninhaber und Datennutzer. Interessenkonflikte sind zu vermeiden. Die Entscheidungen erfolgen weisungsfrei (Art. 36 Abs. 3). Diese Regeln sind zwar enger als die für das deutsche Forschungsdatenzentrum, wo die Entscheidungen durch eine dem Bundesgesundheitsministerium nachgeordnete Behörde erfolgen. Doch genügen die Festlegungen nicht, um qualifizierte unabhängige Entscheidungen mit den hochsensitiven Daten sicherzustellen.

Allmächtige Kommission

Unabhängigkeit bedeutet insbesondere auch Unabhängigkeit von der Exekutive, d.h. auf europäischer Ebene von der Administration der EU-Kommission. Es wäre unerträglich, wenn die Exekutive durch ihre normativen Vorgaben den Umgang mit den sensitiven Gesundheitsdaten unkontrolliert vorgeben könnte. Die Kommission soll beim EHDS durch delegierte Rechtsakte gemäß Art. 67 Folgendes bestimmen können:

- Festlegung der prioritär bereitzustellenden Gesundheitsdaten (Art. 5 Abs. 2),
- Zusätzliche Aufgaben der nationalen digitalen Gesundheitsbehörden (Art. 10 Abs. 3),
- Befreiung von den analogen Informationspflichten über EHR-Systeme und Wellnessprodukte (Art. 25 Abs. 3),
- Festlegung der digitalen Informationspflichten für EHR-Systeme und der registrierungsfähigen Wellness-Produkte (Art. 32 Abs. 4),
- Erweiterung der Mindestkategorien zur Daten-Sekundärnutzung (Art. 33 Abs. 7),
- Änderung der Aufgabenliste für Zugangsstellen (Art. 37 Abs. 4),
- Änderung der jährlichen Publikationspflicht der Zugangsstellen (Art. 39 Abs. 3),
- Änderung der Bereitstellungspflichten der Dateninhaber (Art. 41 Abs. 7),
- Änderung der Pflichtenliste für Zugangsanträge (Art. 45 Abs. 7),
- Änderung der zu erfassenden Merkmale von Zugangsgenehmigungen (Art. 46 Abs. 8),
- Änderung der Kategorien für HealthData@EU-Teilnehmer (Art. 52 Abs. 7),
- Änderung der technischen Merkmale und Spezifikationen der Datenqualitäts- und -nutzenlabels (Art. 56 Abs. 4).

Der Kommission würden damit sehr weitgehende Befugnisse zur Modifikation des EHDS mit hoher Grundrechtsrelevanz eingeräumt. Dem EU-Parlament und dem EU-Rat wird lediglich ein befristetes Veto-Recht zugestanden (Art. 67 Abs. 6). Es bedarf einer vertieften Prüfung, inwieweit damit die europäischen Gesetzgebungsbefugnisse von Rat und

Parlament beschnitten werden und inwieweit dadurch nationale Gesetzgebungskompetenzen tangiert werden. Angesichts der schon bestehenden Weite der im EHDS-E vorgesehenen Übermittlungspflichten ist eine Befugnisausweitung durch delegierte Rechtsakte kaum vermittelbar. Richtig ist wohl, dass Beschränkungen hinsichtlich des umfangreichen Datenkranzes sinnvoll sind, insbesondere während der Einführungs- und Konsolidierungsphase des EHDS. Angesichts der Dynamik der Digitalisierung des europäischen Gesundheitswesens ist eine gewisse normative Flexibilität sinnvoll. Dadurch darf aber nicht der Wesentlichkeitsgrundsatz bei Eingriffsbefugnissen in Grundrechtspositionen aufgegeben werden.

Fazit

Der EHDS ist ein hochambitioniertes Gesetzgebungsverfahren mit hoher Relevanz für die Gesundheitssysteme in den EU-Mitgliedstaaten und für die Grundrechte der Betroffenen. Die damit verfolgten Anliegen sind berechtigt. Die konkrete Ausgestaltung bedarf aber in vieler Hinsicht noch der intensiven Diskussion und Korrektur. Insofern ist nicht damit zu rechnen, dass über dieses Gesetzgebungsvorhaben kurzfristig Einigkeit hergestellt wird. Qualität ist wichtiger als Schnelligkeit. Zugleich muss das Gesetzgebungsverfahren von technischen Entwicklungen und Standardisierungen begleitet werden, ohne die der EHDS ein Papiertiger bleiben würde.

Die normativ vorzugebende und in der Praxis zu lösende Aufgabe, die Abwägung zwischen den Datenschutzinteressen und den öffentlichen Interessen an der Sekundärnutzung grundrechtskonform zu gestalten, ist weder im deutschen DVG noch im EHDS-E befriedigend geregelt. Entsprechende Vorgaben könnten auch in den von den Koalitionspartnern angekündigten Gesetzen zu Forschungsdaten und zur Gesundheitsdatennutzung erfolgen. Diese Vorgaben müssen u.a. folgende Aspekte konkret sicherstellen:

- Materielle Festlegungen zur Grundrechtswertigkeit der eingesetzten Gesundheitsdaten wie der öffentlichen Nutzungsinteressen,
- prozedurale Vorgaben zur Anonymisierung, zur Aggregierung und zur Pseudonymisierung,
- Festlegungen zur Besetzung und zur Entscheidungsfindung der Zugangsstellen, um unabhängige und qualifizierte Entscheidungen zum Datenzugang sicherzustellen,
- strafbewehrtes Reidentifizierungs- und Zweckentfremdungsverbot,
- privilegierende Sonderregelungen für die unabhängige wissenschaftliche Forschung,
- Einführung eines beschlagnahmefesten Forschungsgeheimnisses[37],
- Datentransparenz für die Betroffenen,
- zeitnahe öffentliche Transparenz über Antragstellung und Zugangsgewährung,
- Etablierung eines Prozesses zur Wahrnehmung der Betroffenenrechte, insbesondere des Auskunfts- und des Widerspruchsrechts,
- technische Absicherung der Kommunikations- und Verarbeitungsprozesse,
- unabhängige Aufsicht über die Entscheidungen der Zugangsstellen und regelmäßige Kontroll- und Stichprobenverfahren mit sofortiger Interventionsmöglichkeit.[38]

Die regulative Aufgabe ist – angesichts des ambitionierten Vorhabens – eine große Herausforderung. Dabei muss darauf geachtet werden, dass mit den Regeln kein bürokratisches Monster entsteht, mit dem sinnvolle Sekundärnutzungen faktisch verhindert werden. Der EU-Kommission kann das Kompliment gemacht werden einen Entwurf vorgelegt zu haben, der umfassend und strukturell gut durchdacht ist. Mit ihm ist es möglich, die heterogenen nationalen Landschaften der Verarbeitung von Gesundheitsdaten in der EU zusammenzuführen, ohne diesen mit ihren Besonderheiten und Qualitäten übermäßig Gewalt anzutun.

Der EHDS-E ist aber nicht mehr als ein Entwurf, der noch auf den Feinschliff wartet. Dieser kann und muss in vieler Hinsicht auf EU-Ebene erfolgen. Die Hauptaufgabe bleibt aber insofern bei den Mitgliedstaaten. Diese müssen ihre gewachsenen Gesundheitssysteme an die geplante Kooperationsstruktur anpassen. Diese Aufgabe kann in Deutschland durch die im Koalitionsvertrag angekündigten Gesetze zu Forschungsdaten und zur Gesundheitsdatennutzung in Angriff genommen werden. Mit einer zeitnahen Gesetzgebung kann der deutsche Gesetzgeber zugleich gestaltenden Einfluss auf die weitere Diskussion zum EHDS nehmen. Parallel dazu muss die Praxis der Gesundheitsdatenverarbeitung sich darauf einstellen, dass mit dem durch den EHDS erfolgenden Paradigmenwechsel schon heute Modifikationen angebracht sind.

1 Das englische Kürzel wird auch in deutscher Sprache verwendet, im Folgenden wird der Entwurf als EHDS-E abgekürzt; Regelungszitate mit Art. oder ErwGr ohne andere Beschreibung beziehen sich hierauf.

2 Europäische Kommission, Europäische Datenstrategie (2020). https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_de.

3 Kommission, Eine europäische Datenstrategie v. 19.02.2020, COM(2020) 66 final.

4 Raji ZD2023, 4.

5 Kritisch zu der Verwendung zweier unterschiedlicher Begriffe Petr DuD 2022, 416.

6 Richtlinie 2011/24/EU v. 09.09.2011, ABl. L 88 v. 4.4.2011, S. 45.

7 Verordnung (EU) 2017/745 v. 05.04.2017 über Medizinprodukte, ABl. L 117 v. 05.05.2017, S. 1.

8 Verordnung (EU) 2017/746 v. 05.04.2017 über In-vitro-Diagnostika, ABl. L 117 vom 5.5.2017, S. 176.

9 Verordnung (EU) 2021/953 v. 14.06.2021 über einen Rahmen für die Ausstellung, Überprüfung und Anerkennung interoperabler Zertifikate zur Bescheinigung von COVID-19-Impfungen und -Tests sowie der Genesung von einer COVID-19-Infektion, ABl. L 211/1 v. 15.06.2021.

10 Verordnung (EU) 2022/868 v. 30.05.2022, ABl. EU L v. 03.06.2022, L 152/1.

11 EU-Kommission, 23.02.2022 COM(2022) 68 final, 2022/0047 (COD).

12 Verordnung (EU) 2021/522 v. 24.03.2021, ABl. L 107/1 v. 36.03.2021.

13 Petri DuD 2022, 416; kritisch Raji ZD 2023, 7.

14 Zu der unklaren Abgrenzung zwischen personenbezogenen und nicht-personenbezogenen Gesundheitsdaten Petri DuD 2022,415.

15 DVG v. 09.12.2019, BGBl. I S. 2562.

16 Raji ZD 2023, 6.

17 Weichert, Datenschutzrechtliche Rahmenbedingungen medizinischer Forschung, 2022, S. 34 ff.

18 Weichert, Rahmenbedingungen (En. 17), S. 108 f.

19 Datenethikkommission, Gutachten 2019, S. 124 f.; ebenso Ethikrats-Vorsitzende Buyx in: Bernd, „Das kostet Leben", SZ 09.12.2022, 12.

20 Sachverständigenrat, Digitalisierung für Gesundheit, 2021, XXVII (Rn. 23).

21 Koalitionsvertrag, Mehr Fortschritt wagen, 2021, S. 21, 83, dok. in DANA 1/2022, 20 f.

22 Stellungnahme „Das Gesundheitsdaten-Ermächtigungsgesetz der EU-Kommission", https://patientenrechte-datenschutz.de/ehds-stellungnahme/; ähnlich MdEP Breyer, Pressrelease 08.11.2022, European Health Data Space: Threat to self-determination and privacy.

23 Art. 33 Abs. 1 lit. c u. e EHDS-E.

24 Kritisch Raji ZD 2023, 7; Petri DuD 2022, 418.

25 Weichert MedR 542 f.; Weichert DANA 1/2020, 23 f.; Weichert FIfF-Ko 2/2020, 39.

26 Petri DuD 2022, 418.

27 Krempl, EU-Gesundheitsdatenraum: Bundesrat für Widerspruchsrecht vor Forschungsfreigabe, www.heise.de 16.09.2022, Kurzlink: https://heise.de/-7267091.

28 Weichert ZD 2020, 23; Weichert Rahmenbedingungen (En. 17), 108 f.

29 Raji ZD 2023, 7; Petri DuD 2022, 418.

30 Weichert MedR 2020, 544 ff.

31 Ähnlich Cimina, vom EDPS zit. in Krempl, EU-Gesundheitsdatenraum: Patientendaten-Freigabe für Sekundärdaten umkämpft, www.heise.de 30.11.2022, Kurzlink: https://heise.de/-7361089.

32 Weichert, Rahmenbedingungen (En. 17), S. 34 ff.

33 Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK), Petersberger Erklärung v. 24.11.2022.

34 Weichert MedR 2020, 544.

35 BVerfG 29.05.1973 – 1 BvR 424/72 u. 325/72 Rn. 128; dies aufgreifend § 38a AufenthV; Weichert ZD 2020, 19; ausführlich Weichert, Rahmenbedingungen S. 18 ff.

36 Weichert ZD 2020, 19 f.; Weichert, Rahmenbedingungen S. 20 f. m.w.N.

37 DSK, Petersberger Erklärung v. 24.11.2022 (En. 33), Nr. 6.

38 DSK, Petersberger Erklärung v. 24.11.2022 (En. 33), Nr. 7.

Ulrich Kelber

Digitalisierung und Datenschutz: Schluss mit Ausreden!

Wenn es bei der Digitalisierung hakt, zeigen die Finger schnell auf den Datenschutz als vermeintliche Bremse. Damit muss Schluss sein, kommentiert der Bundesdatenschutzbeauftragte Ulrich Kelber – damit der Blick auf die echten Hindernisse frei wird.

Prof. Dipl.-Inf. Ulrich Kelber ist seit 2019 der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Von 2000-2018 war er Mitglied des Deutschen Bundestags und von 2013-2018 parlamentarischer Staatssekretär beim Bundesminister der Justiz und für Verbraucherschutz. Er ist Mitglied im Executive Commitee der Weltvereinigung der Datenschutzbehörden und Vorsitzender der International Working Group on Data Protection in Technology.

Deutschland braucht einen Digitalisierungsschub. Egal, ob in der Verwaltung, im Gesundheitswesen, bei der Mobilität oder im Bildungsbereich. Doch wenn es bei Projekten wie eID, digitaler Gesundheitsdokumentation, Registermodernisierung oder Bildungsplattformen nicht läuft, ist der vermeintlich Schuldige schnell gefunden: der Datenschutz.

Unkonkrete und nie belegte Schuldzuweisungen an den Datenschutz haben sich in Talkshows, in Reden auf Konferenzen, Gastbeiträgen in Medien und einigen Leitartikeln durchgesetzt. Das ist einfach nur traurig und führt in eine Sackgasse des Denkens. Und das, obwohl es doch eigentlich darum geht, die erschreckenden Mängel in der Digitalisierung in Deutschland abzustellen. Dafür müssen sich alle Beteiligten auch bei widerstreitenden wirtschaftlichen Interessen zusammentun.

Eine behauptete überzogene Regulierung in Deutschland und eine angebliche besonders strenge deutsche Auslegung der europaweit geltenden Datenschutzgrundverordnung existieren nachweisbar nicht. Im Gegenteil, meist sind die Erzählungen vom hinderlichen Datenschutz leicht faktisch widerlegbar. Doch das hält die Akteure nicht davon ab, sie regelmäßig zu wiederholen.

Ein besonders absurdes Beispiel ist der Gesundheitssektor, wo sich die Extreme schmerzhaft zeigen: Die unzureichende Digitalisierung und föderale Unterschiede in der Gesetzgebung führen dazu, dass hilfreiche Daten bis heute nicht erhoben oder zu wenig genutzt werden. Das schadet insbesondere den Patientinnen und Patienten. Denn so können nicht alle Möglichkeiten der Forschung genutzt werden, es lagen nicht genügend Erkenntnisse etwa über den Verlauf der Corona-Pandemie vor, Doppeluntersuchungen werden notwendig oder es kommt zu Fehlmedikationen.

Werden IT-Sicherheit und Datenschutz im Gesundheitssektor nicht ausreichend berücksichtigt, können die besonders sensiblen Gesundheits-

daten andererseits leicht in falsche Hände geraten. Die teils sehr unangenehmen Konsequenzen für die Betroffenen von Hacks oder Leaks finden in der öffentlichen Diskussion viel zu wenig Beachtung.

Ethikrat, gematik, Krankenkassen und Verbände: das gleiche Muster

Ich unterstütze die eindringliche Forderung des Deutschen Ethikrats, dass die Digitalisierung des Gesundheitssektors endlich vorankommen muss, um den Patientinnen und Patienten bestmögliche Hilfe zu geben. Aber statt die zwanzig Jahre Verzögerung bei Projekten, inkompatible Datenformate, unzureichende Meldewege, mangelnde Softwarequalität und die gegenseitige Blockade der Interessensgruppen anzuprangern, arbeitet sich der Ethikrat einseitig am Datenschutz ab und lässt dabei oft genug grundlegende Faktenkenntnis vermissen.

Besonders unerträglich war das Verhalten des stellvertretenden Vorsitzenden des Ethikrates, Nida-Rümelin, in den Hochzeiten der Corona-Pandemie. Da zog er von Talkshow zu Talkshow und behauptete, die Datenschützer seien schuld an zehntausenden Toten und hunderttausenden vernichteten Existenzen, weil sie eine „zahnlose Corona-Warn-App“ erzwungen hätten. Man müsse sich stattdessen an den Apps in Südkorea, Japan und Taiwan orientieren.

Doch obwohl die drei genannten Staaten gar keine besseren Gesamt-Infektionszahlen als Deutschland hatten und haben, wiederholte Nieda-Rümelin seine Behauptung bis zuletzt; selbst nachdem er mehrfach über die grundlegenden Fakten informierte wurde: Südkorea verwendet seine App nicht zur Kontaktverfolgung, Japan nutzt exakt die gleiche Technologie wie Deutschland und Taiwan hat gar keine App in diesem Bereich.

Ein Beispiel für faule Ausreden bei verschleppter Digitalisierung liefert leider die gematik. Das Unternehmen ist sozusagen das IT-Haus des Bundes für den Gesundheitssektor. Und sie schiebt immer noch – auch wenn sie sich in zunehmend besseren Strukturen um ihre Aufgaben kümmert – gerne den Anforderungen von IT-Sicherheit und Datenschutz die Schuld für zum Teil seit Jahren verzögerte Projekte zu.

Zuletzt behauptete der Bereichsleiter eHealth & gematik des Bundesgesundheitsministeriums im Januar in einem Interview, man brauche eine bessere Abwägung zwischen IT-Sicherheits- und Datenschutzanforderungen auf der einen Seite und gut nutzbarer Digitalisierung auf der anderen Seite. Worauf er anspielte: Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) und meine Behörde, der BfDI, hatten den gematik-Vorschlag für eine von mehreren Einreichungsformen von eRezepten abgelehnt.

Was er nicht erwähnte: Der abgelehnte Entwurf hätte es mit minimalem Aufwand ermöglicht, in mehr als 18.000 Einrichtungen unrechtmäßig in die Rezeptdaten aller(!) Krankenversicherten Einblick nehmen und damit Rückschlüsse auf Krankheiten aller Art ziehen zu können. Übrigens: BSI und BfDI haben natürlich nicht einfach „Nein“ gesagt, sondern aufgezeigt, wie man die scheunentorgroße Sicherheitslücke in einer Form schließt, die exakt die gleiche Bedienung bei voller Sicherheit ermöglicht. Auf die krude Idee, Nutzungskomfort gegen Sicherheit und Grundrechtsschutz auszuspielen, statt beides zu bieten, muss man erst einmal kommen.

Ein weiterer Fall sind die Krankenkassen und einige Verbände, die ihre eigenen Interessen auch dadurch verfolgen, dass sie gegen IT-Sicherheit und Datenschutz schießen, sehr wohl zum Nachteil der Versicherten und bis hin zur Gefährdung von Patientenwohl. Die Krankenkassen statten ihre Versicherten zum Beispiel nicht mit einer PIN für deren elektronische Gesundheitskarte aus. Mit eGK und PIN könnten diese sich aber sicher unter anderem bei der elektronischen Patientenakte anmelden oder eRezepte in der Apotheke einlösen.

Stattdessen fordern die Krankenkassen immer wieder die Zulassung weniger sicherer Technologien zur Authentifizierung, zuletzt warb die Techniker Krankenkasse sogar bei Nutzer:innen ihrer App, die sich für die sichere Authentifizierung mit eGK entschieden hatten, dafür, doch auf die weniger sichere, von BSI und BfDI nur noch übergangsweise geduldete Variante ohne eGK umzusteigen. Man stelle sich vor, die Banken würden es ihren Kunden besonders schwierig machen, Bankkarten mit PIN zu nutzen und wieder zur Unterschrift auf dem Scheck zurückkehren wollen.

Besonders ärgerlich sind auch die Versuche, eigene Interessen an ganz anderer Stelle durch Kritik an IT-Sicherheit und Datenschutz durchzusetzen. Ein besonders schlimmes Beispiel war der Generalsekretär der Deutschen Gesellschaft für Orthopädie und Unfallchirurgie (DGOU), der behauptete, man dürfe die Gesundheitsdaten eines bewusstlosen Patienten im Rettungswagen nicht an das angefahrene Krankenhaus vorab übermitteln, weil ja die Einwilligung des Patienten fehle. Der Datenschutz in diesem Bereich müsse heruntergesetzt werden, forderte er. Man kann nur hoffen, dass kein Notarzt diesen gefährlichen Quatsch gelesen hat.

Auf genau der gleichen Grundlage, auf der man lebensrettende medizinische Maßnahmen wie beispielsweise Luftröhrenschnitte an einem bewusstlosen Patienten im Rettungswagen vornehmen darf, kann man natürlich auch die Daten an das behandelnde Krankenhaus geben. Alles das weiß der Verband, der auf der anderen Seite aber tatsächlich ein verbandsinternes Datenschutzproblem hat: Er wünscht sich die verpflichtende Einspeisung aller solcher Daten in bestimmten medizinischen Fällen in sein auf privatrechtlicher Basis betriebenes Register. Das geht aber nur mit einer gesetzlichen Grundlage, wie sie es zum Beispiel beim Implantateregister gibt.

Bündnis für schnellere Digitalisierung

Ähnliche Beispiele wie aus dem Gesundheitssektor findet man auch in anderen Bereichen. Die einen beschweren sich über die Anforderungen von IT-Sicherheit und Datenschutz, um über eigene Versäumnisse, Minderleistungen und Unkenntnisse hinwegzutäuschen. Die anderen nutzen die völlig berechtigte Debatte über die schwache Digitalisierung in Deutschland, um gegen IT-Sicherheits- und Datenschutz-

regelungen zu schießen, die angeblich wichtige Geschäftsmodelle verhindern. Dabei sind es in Wirklichkeit Geschäftsmodelle, die die Bürgerinnen und Bürger benachteiligen, wie etwa das massenhafte Sammeln von Verhaltensdaten der Kunden.

Was wir brauchen, ist ein Bündnis für schnelle Digitalisierung, das Lösungen voranbringt, denen die Bürgerinnen und Bürger vertrauen können. Dafür sind Sicherheit und Schutz der Daten unabdingbare Voraussetzungen. Ein Bündnis, dass sich gegen das Lamentieren in den Talkshows stellt. Und damit Handelnde darin bestärkt, legale und mögliche Datenverarbeitungen auch durchzuführen. Ein Bündnis, bei dem alle Seiten anerkennen, dass die verschiedenen Grundrechte nicht gegeneinanderstehen. Ein Bündnis, das versteht, dass gute Lösungen möglich sind, wenn die Beteiligten von Anfang an miteinander sprechen und zusammenarbeiten.

Wenn also alle wichtigen Akteure endlich aufhören würden, sich am gefährlichen Narrativ des bösen Datenschutzes abzuarbeiten, würde der Blick frei auf die echten Hindernisse der Digitalisierung.

Man hätte ein starkes Bündnis, das sich für ebenso starke Lösungen bei grundlegenden Projekten einsetzen könnte, wie etwa der eID, den digitalen Gesundheitsdokumentationen, der Modernisierung staatlicher Register, funktionierenden Bildungsplattformen und der Nutzung wichtiger Daten für das Gemeinwohl.

Dazu müssen selbstverständlich auch die Datenschutzaufsichtsbehörden einen Beitrag leisten: Mit engagierter Beratung und modernisierten eigenen Strukturen, um noch schneller abgestimmte Antworten der deutschen und europäischen Aufsichtsbehörden zu wichtigen rechtlichen und technischen Fragestellungen geben zu können, wie beispielsweise mit unserer Petersberger Erklärung vom November 2022 zur Nutzung von Gesundheitsdaten zu Forschungszwecken.

Wir Datenschutzbehörden wollen zeigen, dass für uns alle Grundrechte gleichrangig sind und wir nicht nur die informationelle Selbstbestimmung im Blick haben, denn das setzen wir täglich in der Praxis um.

Wir Datenschutzaufsichtsbehörden halten dafür unser uneingeschränktes Dialogangebot an alle Beteiligten aufrecht. Deshalb freue ich mich sehr, dass mein immer wieder erneuertes Angebot für einen persönlichen Austausch zu diesen Fragen vom Ethikrat nun endlich angenommen wurde. Packen wir es an!

(Dieser Text wurde am 04.02.2023 als Gastbeitrag vom BfDI Prof. Ulrich Kelber auf https://netzpolitik.org/2023/digitalisierung-und-datenschutz-schluss-mit-ausreden/ abgedruckt und steht unter der Lizenz CC BY-NC-SA 4.0: „Lizenz: Die von uns verfassten Inhalte stehen, soweit nicht anders vermerkt, unter der Lizenz Creative Commons BY-NC-SA 4.0.“)

Presseerklärung der DVD – Bonn, 15.12.2022

Datenschützer: Registerkorrekturen müssen umgehend erfolgen

Die Deutsche Vereinigung für Datenschutz e.V. (DVD) macht auf ein umfangreiches Gutachten ihres Vorstandsmitglieds Thilo Weichert aufmerksam, in dem die seit August 2022 erfolgende Veröffentlichung von Daten des Vereins-, des Handels-, des Genossenschafts- und der Partnerschaftsregister unter www.handelsregister.de rechtlich hinterfragt wird.

Das Gutachten kommt zu dem Ergebnis, dass die derzeitige Preisgabe von personenbezogenen Daten von Vereinsvorständen und Vertretungsberechtigten von Unternehmen im Internet weitgehend nicht erforderlich und deshalb unzulässig ist. Sensible Angaben zur Geburt, zur Wohnung, zur Kontoverbindung oder gar Originalunterschriften können zum Identitätsdiebstahl und für sonstige kriminelle Machenschaften missbraucht werden.

Die DVD bietet auf ihrer Webseite einen Formulartext an, mit dem Betroffene sich gegen eine Veröffentlichung ihrer Daten zur Wehr setzen können. In einem Hinweisblatt werden praktische Ratschläge gegeben, wie Betroffene ihre Rechte und insbesondere ihr Widerspruchsrecht gegen die Veröffentlichung geltend machen können (https://www.datenschutzverein.de/hinweisblatthandelsregister/).

Entgegen den ausdrücklichen gesetzlichen Einschränkungen der Betroffenenrechte hat das Bundesjustizministerium schon signalisiert, dass den Betroffenen ein Widerspruchsrecht sowie die Möglichkeit des Austauschs von Daten zusteht. Dieses Eingeständnis geht der DVD nicht weit genug, wie das Rechtsgutachten dargelegt:

- Da für die Registerveröffentlichung nicht nur die Registergerichte, sondern auch das Landesjustizministerium Nordrhein-Westfalen rechtlich verantwortlich ist, können sämtliche Betroffenenrechte gegenüber dem Ministerium geltend gemacht werden.
- Aus Publizitätsgründen nicht erforderlich und deshalb von der Veröffentlichung auszuschließen sind sensible Angaben von Vertretern von Gesellschaften wie die Unterschrift und das Geburtsdatum. Von Vereinsvorständen veröffentlicht werden dürfen nur die Namen und der Wohnort, wenn die Vorstandstätigkeit aktuell besteht oder maximal 3 Jahre zurückliegt.
- Ein Ausschluss von der Veröffentlichung setzt nicht voraus, dass zuvor die der Registrierung zugrundeliegenden notariellen Dokumente bereinigt und ausgetauscht werden; die Bereinigung kann und muss vielmehr von den Registergerichten vorgenommen werden.
- Es ist wohl nicht zu beanstanden, dass www.handelsregister.de weiterhin online ist. Unabdingbar ist aber, dass individuelle Widersprüche vom Landesjustizministerium und vom Registergericht einzelfallbezogen behandelt werden und bei fehlender Publizitätserforderlichkeit von der Veröffentlichung ausgenommen werden.

DVD-Vorstandsmitglied und Autor des Gutachtens Thilo Weichert: „Es ist ein Trauerspiel, wie sich bisher alle Verantwortlichen – einschließlich der zuständigen Datenschutzaufsicht – aus ihrer datenschutzrechtlichen Verantwortung stehlen und dass dadurch die von staatlicher Seite veröffentlichten sensiblen Daten jedermann zum Identitätsdiebstahl zur Verfügung gestellt werden."

DVD-Vorsitzender Frank Spaeing ergänzt: „Die Politik muss tätig werden. Die rechtlichen Register-Grundlagen, welche gegen Verfassungs- und Europarecht verstoßen, sind insgesamt zu überarbeiten. Betroffene müssen transparent erkennen können, was mit ihren Daten geschieht. Nur solche Daten dürfen über das Internet veröffentlicht werden, die zur Herstellung der Rechtssicherheit im Wirtschaftsleben unbedingt nötig sind."

Offizielle Reaktionen – was bisher (noch nicht) geschah

Die DVD und das Netzwerk Datenschutzexpertise (welches das Gutachten zur Registerveröffentlichung im Internet verfügbar macht) wandten sich an die für den Datenschutz in Nordrhein-Westfalen zuständige Aufsichtsbehörde, die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI NRW), in der Erwartung, dass diese das Anliegen der DVD unterstützt. Sie wandten sich zudem an das Justizministerium Nordrhein-Westfalen (MJ NRW), das für den Betrieb des Registerportals beim Amtsgericht Hagen verantwortlich ist. Das MJ NRW antwortete und gab die (auch einen konkreten Verein betreffende) Anfrage teilweise an das (zuständige) Registergericht, das Amtsgericht Kiel, weiter, das auch antwortete. Im Folgenden werden Auszüge aus den Antworten dokumentiert.

• LDI NRW

Die Antwort der LDI NRW vom 19.12.2022 ist eher enttäuschend:

„Ich kann Ihnen versichern, dass wir uns insbesondere mit der Frage, ob eine justizielle Tätigkeit vorliegt oder nicht, intensiv auseinandergesetzt und auch mit dem AK Justiz abgestimmt haben. Selbst wenn man der Einschätzung des Gutachtens folgen wollte, weist der Kommentar, auf den sich das Gutachten stützt, auf die unbedingt zu wahrende richterliche Unabhängigkeit hin. Insoweit bestünde auch nach der dort vertretenen Auffassung eine praktisch nicht aufzulösende rechtliche Pattsituation.

Des Weiteren ist nach unseren tatsächlichen Feststellungen bei der vorliegenden Konstellation keine ge-

meinsame Verantwortlichkeit für die inhaltlichen Daten gegeben. Sowohl die Veröffentlichungspflicht, als auch das Führen der Register liegen ausschließlich in der Verantwortung der jeweiligen Gerichte. In Hagen wird nur der technische Rahmen zur Verfügung gestellt, mittels dessen die jeweiligen Gerichte ihrer Veröffentlichungspflicht nachkommen können. Auch hier können wir der Sicht des Gutachtens nicht folgen.

Unabhängig davon bin ich in engem Austausch mit unserem Justizministerium, um ungeachtet der Kontrollzuständigkeiten auf eine datenschutzkonforme Lösung zu drängen. Ich teile Ihre Auffassung, dass eine zügige Lösung im Interesse der Betroffenen wäre. Doch diese werde ich bei unklarer Rechtslage und mit Maßnahmen, die ich nicht unmittelbar vollziehen kann, kaum erreichen. Daher hoffe ich auf eine schnellere Lösung im Konsens mit der Justiz."

• MJ NRW

Das Ministerium der Justiz des Landes Nordrhein-Westfalen (MJ NRW) reagierte auf die Forderung nach Bereinigung der im Internet veröffentlichten Vereinsregister mit Schreiben vom 18.01.2023 wie folgt (Az. 1511E-IT/Justizportal 2023):

„Durch das Ministerium der Justiz des Landes Nordrhein-Westfalen wird nur die technische Infrastruktur für den Betrieb des gemeinsamen Registerportals der Länder bereitgestellt. Das gemeinsame Registerportal dient der zentralen Einsichtnahme in die bei den jeweiligen Registergerichten geführten Register (Handelsregister, Genossenschaftsregister, Vereinsregister etc.). Bei einem Abruf werden die Daten der lokalen Register zur Einsichtnahme bereitgestellt. Das gemeinsame Registerportal hält die Daten weder selbst vor, noch hat es die Datenhoheit. Letztere liegt bei den jeweiligen Registergerichten.
[...]

Zunächst möchte ich darauf hinweisen, dass sich der vertretungsberechtigte Vorstand eindeutig aus dem Vereinsregister ergeben muss. Im Rechtsverkehr vertritt der Vorstand den Verein im Außenverhältnis. Dies macht erforderlich, dass jeder Vorstand zweifelsfrei und eindeutig identifiziert werden können muss. Dies gilt im Übrigen auch für die Vergangenheit, nicht nur für die Gegenwart. Insoweit sei auf § 67 BGB und § 3 S. 2 Nr. 3 Vereinsregisterverordnung (VRV) verwiesen. Diese Vorschriften sehen vor, dass in Spalte 3 unter Buchstabe a die allgemeine Vertretungsregelung und unter Buchstabe b die Vertretungsberechtigten (der Vorstand und etwaige Liquidatoren) mit Namen, Vornamen, Wohnort, Geburtsdatum und, soweit zweckmäßig, auch die Stellung im Vorstand sowie besondere Vertretungsbefugnisse sowie die Änderung dieser Eintragungen unter kurzer Angabe des Grundes einzutragen sind. Demzufolge ist die Eintragung [...] als Vorstand unter Angabe von Vor- und Zunamen sowie Geburtsdatum aus diesseitiger Sicht nicht zu beanstanden, sondern auch gesetzlich vorgeschrieben.

Um die Registerpublizität und die eindeutige Identifizierbarkeit im Rechtsverkehr herzustellen, gilt die DSGVO gem. § 79a BGB in Bezug auf das Vereinsregister nur eingeschränkt. Insbesondere sieht § 79a Abs. 3 BGB vor, dass das Widerspruchsrecht gem. Art. 21 DSGVO nicht anzuwenden ist. Entgegen Ihrer Auffassung kann damit der Veröffentlichung nicht widersprochen werden.

In diesem Zusammenhang darf ich noch darauf hinweisen, dass diese Form der Beauskunftung schon seit Bestehen des gemeinsamen Registers erfolgt ist. Weggefallen ist lediglich zum 01.08.2022 die Kostenpflicht von 1,50 EUR bzw. 4,50 EUR für die entsprechenden Auskünfte. Vorfälle von Identitätsdiebstahl sind mir weder in der Vergangenheit noch jetzt bekannt geworden.

Da die Datenhoheit nicht bei mir liegt, sondern beim Amtsgericht [...], sind mir Maßnahmen in Bezug auf die Art und Weise der veröffentlichten Daten verwehrt. [...] Nur das Amtsgericht [...] als registerführende Stelle kann entscheiden, ob die Publizierung der Angaben notwendig ist oder nicht.

Ich werde Ihrem Wunsch folgend Ihre Eingabe betreffend den Verein [...] auf dem Dienstweg [...] dem Amtsgericht [...] zukommen lassen. [...]

Da die Gerichte jedoch unabhängig sind, kann ich auf deren Entscheidung und Maßnahmen von hier aus keinen Einfluss ausüben."

• Amtsgericht Kiel

Ein vom MJ NRW weitergegebener Widerspruch eines Betroffenen an das Amtsgericht Kiel (zuständiges Registergericht) wurde von diesem mit Datum vom 30.01.2023 beantwortet (Az. VR 1644 KI). Hier Auszüge aus der Antwort:

„In der Registersache [...] wird zu Ihrem Schreiben vom 11.01.2023 auf § 79a Absatz 3 BGB hingewiesen. Gemäß § 79a Absatz 3 BGB steht nach Art 21 DS-GVO in Bezug auf die im Vereinsregister eingetragenen persönlichen Daten und die zum Vereinsregister einzureichenden Dokumenten Ihnen kein Widerspruchsrecht zu.

Gemäß § 3 Satz 3 Ziffer 3 b) der Vereinsregisterverordnung sind die Vorstandsmitglieder mit Geburtsdatum und Wohnort ins Vereinsregister einzutragen.

Es wird darauf hingewiesen, dass das Registergericht grundsätzlich davon ausgeht, dass die eingereichten Dokumente mit den Anmeldenden abgestimmt sind, eine Veröffentlichung also gewünscht ist. Die Registergerichte sind bei Anmeldung verpflichtet, die eingereichten Urkunden in den Registerordner aufzunehmen, da sie Grundlage für das Eintragungsbegehren waren. Eine Bearbeitung oder Veränderung der Dokumente durch das Registergericht zum Schutz etwaiger Daten ist nicht zulässig. Das Gericht darf eingereichte Urkunden nicht verändern. Die von Notar [...] erstellte Urkunde [...] kann durch eine geänderte Urkunde ersetzt werden. Sie müssen sich dazu an Notar [...] wenden, damit er alles Erforderliche veranlasst und eine Urkunde ohne Ihre vollständige Wohnanschrift einreicht (§ 9 Absatz 7 Handelsregisterverordnung analog).

Gemäß § 67 Absatz 1 BGB ist jede Änderung des Vorstands vom Vorstand zur Eintragung ins Vereinsregister anzumelden. Der Anmeldung ist eine Abschrift der Urkunde über die Änderung beizufügen. Die Angabe des Abstimmungsergebnisses in einer Mitgliederversammlung ist eine Voraussetzung dafür um festzustellen, ob überhaupt eine ordnungsgemäße Wahl erfolgt ist. Daher kommt hier ein Austausch der Urkunde nicht in Betracht."

• **Was daraus folgt**

Die LDI NRW und das Bundesjustizministerium (BMJ) haben offenbar erkannt, dass die seit August 2022 praktizierte Registerveröffentlichung aus Datenschutzsicht ein Problem darstellt. Wann und wie dieses Problem gelöst wird, ist aber nicht absehbar.

Um insofern individuell wie auch generell eine datenschutzkonforme Lösung zu erreichen, werden Betroffene weiterhin ermuntert, sich gegen übergriffige Registerveröffentlichungen – z.B. unter Nutzung der DVD-Vorlage – zur Wehr zu setzen. Zwar erklärt sich das MJ NRW für nicht zuständig, so scheint es aber bereit zu sein die Widersprüche an die jeweils zuständigen Registerbehörden weiterzugeben. Solange keine einheitlichen Vorgaben vom BMJ oder den Justizverwaltungen erfolgen, müssen die Registergerichte individuell entscheiden. Es kann daher nur gehofft werden, dass dies im Sinne des Datenschutzes und der Datensparsamkeit erfolgt.

Die rechtlichen Argumente der LDI NRW, des MJ NRW und des Amtsgerichts Kiel beruhen ausschließlich auf administrativen und gesetzlichen Vorgaben und berücksichtigen nicht übergeordnetes Recht. Das von der DVD und dem Netzwerk Datenschutzexpertise veröffentlichte Rechtsgutachten begründet aber das Widerspruchsrecht der Betroffenen und die Löschpflicht im Register aus übergeordnetem Recht, nämlich dem Grundrecht auf Datenschutz und der europäischen Datenschutz-Grundverordnung. Diese Vorgaben gehen den nationalen Gesetzen und Verwaltungsverordnungen vor und führen dazu, dass diese nicht angewendet werden dürfen.

Daher sollen Betroffene sich durch die Aussagen der Justizverwaltung nicht gehindert sehen ihre Datenschutzrechte – wie von der DVD empfohlen – wahrzunehmen. Inwieweit ein gerichtliches Vorgehen auf dem Klageweg Erfolg haben wird, kann angesichts der unklaren Rechtslage nicht prognostiziert werden. Erfahrungen mit den Registerveröffentlichungen können weiterhin ausgetauscht werden mit
Thilo Weichert,
Waisenhofstraße 41, 24103 Kiel,
weichert@datenschutzverein.de.

Offener Brief vom 29.11.2022

Meinungsfreiheit bei politischer Kommunikation schützen

Sehr geehrter Herr Bundesminister Wissing,
sehr geehrte Frau Bundesministerin Faeser,
sehr geehrte Frau Bundesministerin Lemke,
sehr geehrter Herr Bundesminister Buschmann,

wir schreiben Ihnen heute, um Sie zu ermuntern sich weiterhin stark für Transparenz bei bezahlter politischer Kommunikation einzusetzen. Der Entwurf einer europäischen Verordnung über die Transparenz und das Targeting politischer Werbung zu diesem Thema darf nicht verwässert und zu vage formuliert werden. Wir sind sehr besorgt, dass einige Entwicklungen im Gesetzgebungsprozess ein erhebliches Risiko für den demokratischen Pluralismus und die Meinungsfreiheit bedeuten.

Politische Werbeanzeigen sind ein wichtiger und etablierter Teil von Wahlkämpfen und gesellschaftlichen Willensbildungsprozessen, haben aber auch das Potenzial zu gesellschaftlichen Spaltungen und zur Polarisierung zwischen politischen Lagern beizutragen. Insbesondere die Datensammlung und -verarbeitung für politische Werbezwecke birgt Risiken für die Privatsphäre und freie Meinungsbildung aller Wähler:innen und für die Integrität demokratischer Prozesse wie Wahlen. Der im November 2021 veröffentlichte Vorschlag der Europäischen Kommission ist ein wichtiger Schritt, um diese Risiken online wie auch offline zu adressieren.

Der Kommissionsvorschlag wurde im Rat an einigen Stellen verbessert, weist aber weiterhin drei große Schwachstellen auf, die es kurzfristig zu schließen gilt: Erstens ist es von höchster Bedeutung, dass es durch die Verordnung nicht zu einer Gleichstellung von bezahlter politischer Werbung und unbezahlten politischen Meinungsäußerungen kommt. Dafür muss deutlicher und klarer definiert werden, was als bezahlte Dienstleistung bei politischer Kommunikation gilt. Politische Äußerungen, für deren Erstellung oder Verbreitung nicht bezahlt wird, sollten keinerlei Beschränkungen außer den bereits im Rahmen der Meinungsfreiheit geltenden unterliegen. Andernfalls bestünde das Risiko einer enormen Einschränkung der Möglichkeit der Teilnahme am politischen Diskurs für Individuen und Organisationen.

Zweitens sollte der Rat davon absehen Ausnahmen zu den Targeting-Regeln einzuführen. Wir möchten all jene im Rat unterstützen, die sich bei der zielgenauen Nutzendenansprache (Targeting) für ein ausnahmsloses Verbot der Verwendung besonders sensibler Daten wie etwa zur Weltanschauung, sexueller Orientierung oder Religionszugehörigkeit aussprechen. Anhand solcher und anderer Daten lassen sich Menschen in kleine, homogene Gruppen einteilen, denen gezielt bezahlte Botschaften ausgespielt werden. Das birgt Missbrauchs- und Diskriminierungspotenzial. Die Mehrheit der Menschen lehnt (https://pure.mpg.de/rest/items/

item_3188061_4/component/file_3195148/content) solche personalisierte politische Werbung ab. Zudem fiele die Verordnung, sollte sie Ausnahmen erlauben, hinter die Targeting-Einschränkungen zu sensiblen Daten aus dem kürzlich in Kraft getretenen Digitale-Dienste-Gesetz der EU (DSA) zurück. Deshalb sollte Artikel 12(2) des Verordnungsentwurfs gestrichen werden.

Drittens äußern wir uns besorgt, dass gut gemeinte Sonderregeln für offizielle Kommunikation von Regierungen ungewollte negative Auswirkungen haben können. In der Ratsfassung vom 22.11.2022 sind Teile der Regierungskommunikation von den Regeln ausgenommen. Während es geboten und sinnvoll ist, öffentliche Kommunikation von Regierungen zu ermöglichen, besteht die Gefahr, dass bezahlte Regierungskommunikation gegenüber oppositionellen oder zivilgesellschaftlichen Anzeigen privilegiert wird. Jegliche Ausnahmen von den Regeln der Verordnung sollten so präzise formuliert sein, dass eine solche Bevorzugung verhindert wird.

Wir unterstützen die wichtigen und ehrgeizigen Ziele in Kommission, Rat und Europäischem Parlament zur Transparenz politischer Werbung. Der Rat hat kurzfristig die Möglichkeit sich für diese Ziele starkzumachen, wenn seine Fassung für eine klare Definition und klare Targeting-Regeln eintritt. Wir rufen die Bundesregierung auf sich mit anderen Mitgliedstaaten in den Verhandlungen im Rat dafür einzusetzen.

Mit freundlichen Grüßen
Stiftung Neue Verantwortung e. V.
D64 – Zentrum für Digitalen Fortschritt e. V.
AlgorithmWatch
Deutsche Vereinigung für Datenschutz e.V. (DVD)
Digitale Freiheit e.V.
Digitale Gesellschaft e.V.
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF)
Gesellschaft für Informatik e.V. (GI)
Wikimedia Deutschland e. V.

Link zum offenen Brief und zu den Logos der Organisationen
https://d-64.org/meinungsfreiheit-bei-politischer-kommunikation-schuetzen/

Offener Brief vom 08.11.2022

Für ein striktes Verbot biometrischer Überwachung

24 zivilgesellschaftliche Organisationen, u.a. Digitalcourage, der Chaos Computer Club und AlgorithmWatch, fordern: Biometrische Überwachung muss strikt verboten werden!

Aktuell arbeitet der Rat der EU, in dem die Regierungen der Mitgliedsstaaten vertreten sind, an seiner Position zur sogenannten KI-Verordnung. Die aktuelle Fassung weist noch große Schlupflöcher auf, die eine Überwachung mittels biometrischer Identifizierungsverfahren im öffentlichen Raum ermöglichen würden.

Im Koalitionsvertrag hat die Bundesregierung ein striktes Verbot biometrischer Überwachung verankert. Die unterzeichnenden zivilgesellschaftlichen Organisationen fordern die deutsche Regierung auf konsequent an ihrer Position festzuhalten und sich für ein umfassendes Verbot biometrischer Überwachung einzusetzen!

Sehr geehrte Mitglieder der deutschen Bundesregierung,

Wir wenden uns an Sie im Namen von 24 zivilgesellschaftlichen Organisationen anlässlich der Verhandlungen zur europäischen Verordnung über Künstliche Intelligenz (KI-Verordnung), die in vollem Gange sind und bezüglich derer sich der EU-Rat demnächst auf eine allgemeine Ausrichtung einigen wird.

Die unterzeichnenden Organisationen begrüßen es sehr, dass die Bundesregierung in ihrem Koalitionsvertrag explizit festgehalten hat, dass biometrische Identifikation im öffentlichen Raum durch eine EU-weite Gesetzgebung ausgeschlossen werden muss. Die KI-Verordnung und insbesondere der Artikel 5d des Entwurfes könnten mit ihren zusätzlichen rechtlichen Absicherungen zu den bereits bestehenden rechtlichen Rahmenbedingungen ein sinnvolles Instrument für ein sinnvolles Verbot werden.

Bedauerlicherweise sehen wir in der letzten Kompromissversion des Rates weiterhin weitgehende Lücken, die ein umfassendes und zuverlässiges Verbot der biometrischen Identifizierung im öffentlichen Raum verhindern würden.

- Erstens betrifft das Verbot in Artikel 5d nur „Echtzeit"-biometrische Identifizierungssysteme in öffentlich zugänglichen Räumen.
- Zweitens ist das Verbot auf Strafverfolgungsbehörden oder in deren Auftrag handelnde Akteure beschränkt – eine Einschränkung, die die Überwachung durch andere öffentliche und private Akteure nicht verhindern würde und die im Koalitionsvertrag so nicht erkennbar ist.
- Drittens sind in den Unterabsätzen im Artikel 5d eine Reihe von Ausnahmen aufgeführt, in denen dieses Verbot nicht gelten sollte, was dessen Gehalt weitgehend aushöhlt.
- Viertens kann die Absicht des EU-Rates, dass die KI-Verordnung nicht anwendbar sein soll, wenn ein Mitgliedstaat sich auf die «nationale Sicherheit» beruft, zur Rechtfertigung des Einsatzes biometrischer Identifizierungssysteme führen, die eine Massenüberwachung ermöglichen können.

In anderen Worten: Das Verbot von biometrischer Überwachung in Art. 5d des KI-Verordnungsentwurfs vermag in seiner aktuellen Form nicht die vielfältigen

Grundrechtsverletzungen, die diese Praktik mit sich bringen kann, zu verhindern.

Wir sehen somit eine Diskrepanz zwischen der im Koalitionsvertrag vertretenen Position und dem, was sich derzeit bei der Ratsposition zur KI-Verordnung abzeichnet. Vor dem Hintergrund der Bemühungen der Bundesregierung für ein Verbot von biometrischer Überwachung im öffentlichen Raum – und damit für die Umsetzung dieses zentralen Koalitionsvertragsversprechens – rufen wir Sie auf sich in dieser entscheidenden Phase der Verhandlungen nochmals explizit dafür stark zu machen. Ein deutliches Signal der deutschen Bundesregierung an die anderen EU-Mitgliedstaaten zum jetzigen Zeitpunkt wäre zentral, um umzusetzen, was die Koalition im Dezember vergangenen Jahres versprochen hat. Das Verbot von biometrischer Überwachung in der KI-Verordnung wird nur dann zuverlässig unsere Grundrechte schützen, wenn dieses nicht voller Schlupflöcher ist. Die europäische Bevölkerung zählt auf Sie.

Unterzeichnende Organisationen:
AlgorithmWatch, AlgorithmWatch Switzerland, Access Now, Amnesty International Deutschland, Article 19, Asociația pentru Tehnologie și Internet, Chaos Computer Club, Citizen D, Digitalcourage, Digitale Freiheit DE, Digitale Gesellschaft, Digitale Gesellschaft CH, ECNL, EDRi, Electronic Frontier Finland, Elektronisk Forpost Norge, epicenter.works, Homo Digitalis, Initiative Schwarze Menschen in Deutschland, Irish Council for Civil Liberties (ICCL), IT-Political Association of Denmark, Open Knowledge Foundation, Reporters Without Borders (RSF) Germany, Wikimedia Deutschland

Herbst 2022, Istanbul, Türkei

Gesichtsüberwachungstechnologie und andere Formen der biometrischen Massenidentifikation verbieten

Wir, die Unterzeichner, fordern ein Verbot der Entwicklung, des Einsatzes und der Nutzung von Gesichtsüberwachungstechnologie und von anderen Formen der biometrischen Massenidentifizierung.

Die Gesichtsüberwachungstechnologie kommt heute zur Identifizierung von Menschen, zur Verhaltensbewertung und für prädiktive Analysen zum Einsatz. Die Auswirkungen der weitgehend unregulierten Technologie sind weitreichend.

Die Gesichtsüberwachungstechnologie kann ganze Stadtgebiete kontrollieren und gleichzeitig die Identität von Zehn- oder Hunderttausenden von Menschen erfassen.

Gesichtsüberwachungstechnologie verstärkt die Identifikationsasymmetrie zwischen Personen und Geräten, wenn sie verborgen mit heimlicher Datenerfassung erfolgt.

Gesichtsüberwachungstechnologie hilft dabei, abweichende Meinungen zu unterdrücken, Minderheiten zu diskriminieren und politische Freiheiten einzuschränken.

Wir nehmen mit Besorgnis aktuelle Berichte zur Kenntnis, wie es bei der Sammlung von Gesichtsbildern zu Voreingenommenheit, Nötigung und Betrug kommt.

Wir erinnern daran, dass die Zivilgesellschaft in der Madrider Erklärung von 2009 ein Moratorium für die Entwicklung und Anwendung von Gesichtserkennung gefordert hat, soweit zuvor keine vollständige und transparente Bewertung durch unabhängige Behörden und in einer demokratischen Debatte erfolgt ist.

Wir erinnern auch an die Erklärung von Tirana aus dem Jahr 2019, in der ein Moratorium für Gesichtserkennungstechnologie im Rahmen von Maßnahmen zu Massenüberwachung gefordert wird.

Und wir erinnern an die Kampagne „ReclaimYourFace", die von 80.000 Einzelpersonen unterstützt wird und in der 76 Organisationen aus 20 europäischen Ländern zusammenarbeiten, die über eine halbe Million Menschen vertreten, um ein Verbot dieser Massenüberwachung zu erreichen.

Deshalb fordern wir die Staaten dringend auf,

- die Entwicklung und den Einsatz von Gesichtsüberwachungstechnologie und anderen Formen der biometrischen Massenidentifizierung zu verbieten,
- alle derzeit verwendeten Gesichtsüberwachungssysteme auf ihre Rechtmäßigkeit hin zu überprüfen und unrechtmäßig erlangte und verarbeitete personenbezogene Daten zu vernichten und
- Untersuchungen zu Bewertung von Voreingenommenheit, Privatsphäre und Datenschutz, zu Risiken und Cyber-Anfälligkeit sowie zu den ethischen, rechtlichen und sozialen Auswirkungen im Zusammenhang mit dem Einsatz von Gesichtsüberwachungstechnologien durchzuführen.

Initial unterzeichnende Einzelpersonen:
Giuliano Borter, CAIDP (Schweiz/Niederlande); Dr. Sivaramakrishnan R Guruvayur, Aaquarians.ai (VAE); Prof. Markus Krebsz, The Human-AI. Institute (Deutschland/Großbritannien); Canan Erez (Deutschland); Victor Famubode (Nigeria); Bisma Shoaib (USA); Saba Elizbarashvili (Georgien); Annett Bonuke (Kenia); Angel Arroyo (Spanien); Dalila Hoover, Esq., CIPP/US/E (USA); Moises Velasco (Spanien); Mélissa M'Raidi-Kechichian (Kanada/Frankreich); Avantika Bhandari (USA);

Nayyara Rahman (Pakistan); Dr. Jordan Richard Schoenherr (Kanada); Mark A. Sayre (USA); Somaieh Nikpoor (Kanada); Alessio Tartaro (Italien); Juliet Murga, Security NextGen (USA); Nicholas Kisundu (Kenia); Marian Ela Ebillo (Philippinen); Roberto López-Dávila (Puerto Rico); Marine Lipartia (Georgien); Unyime Akpabio (Großbritannien); Naciye Busra Memisoglu, Queen Mary University of London (Türkei); Merve Hickok, CAIDP (USA); Marc Rotenberg, CAIDP (USA); Selim Alan (Türkei); Ashkan Alinaghian (Iran); Parisa Osivand (Iran); Rebecca Leeper (USA); Jethro Limjoco (Phillipinen); Omolola Oviroh (Südafrika); Mercy Chinazom Godwin (Nigeria); Dr. Mokesioluwa Fanoro (Südafrika); Gian-Maria Daffré (Schweiz); Dr. Grace S. Thomson (VAE); Prof. Emma Ruttkamp-Bloem, University of Pretoria & Center for AI Research (Südfrika); Dr. Andreas Geppert (Schweiz); Gian-Maria Daffré (Schweiz); Dr. Asli Telli (Deutschland); Ella Jakubowska (Belgien)

Initial unterstützende Organisationen: African Center for AI and Digital Technology (Mauretanien); AI and Digital Ethics Lab, André-Laurendeau College (Kanada); Amnesty International (weltweit); Center for AI and Digital Policy (weltweit); **Deutsche Vereinigung für Datenschutz e.V. (DVD)** (Deutschland); Digitalcourage (Deutschland); Digitale Gesellschaft (Schweiz); Elektronisk Forpost Norge (Norwegen); European Digital Rights (Europa); Homo Digitalis (Griechenland)

Den englischsprachigen Originalaufruf findet sich im Internet unter https://www.caidp.org/statements/ban-facial-surveillance-technology/

10. Januar 2023, Offener Brief zu den

Verhandlungen über ein umfassendes internationales Übereinkommen zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke

Sehr geehrte Frau Vorsitzende H.E. Faouzia Boumaiza Mebarki

Wir, die unterzeichnenden Organisationen und Wissenschaftler, setzen uns online und offline für den Schutz und die Förderung der Menschenrechte ein. Unser gemeinsames Ziel ist es sicherzustellen, dass Menschenrechte und Grundfreiheiten bei der Bekämpfung von Cyberkriminalität, der Sicherung elektronischer Beweismittel, der Erleichterung der internationalen Zusammenarbeit oder der Bereitstellung technischer Hilfe immer Vorrang genießen.

Wir befürchten, dass der vom Ausschuss am 7. November 2022 veröffentlichte Textentwurf mit dem offiziellen Titel „Konsolidiertes Verhandlungsdokument (CND) über die allgemeinen Bestimmungen und die Bestimmungen über die Kriminalisierung sowie über verfahrensrechtliche Maßnahmen und die Strafverfolgung eines umfassenden internationalen Übereinkommens über gegen die Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke“ darauf hinausläuft, gegen internationale Menschenrechte zu verstoßen.

Das CND ist in seinem Umfang zu weit gefasst und nicht auf zentrale Themen der Cyberkriminalität beschränkt. Die CND enthält auch Bestimmungen, die unklar und nichthinreichend präzise sind und Aktivitäten kriminalisieren würden, was nicht mit den Menschenrechtsverpflichtungen der Staaten, die in der Allgemeinen Erklärung der Menschenrechte (UDHR), dem Internationalen Pakt für zivile und politische Rechte (ICCPR) und anderen internationalen Menschenrechtsstandards und -instrumente, niedergelegt sind, in Einklang steht. Im Kapitel des CND zu Strafverfahren und Strafverfolgung fehlen wirksame Menschenrechtsgarantien; zugleich erweitern die materiellen Bestimmungen den Anwendungsbereich auf Absichten und Verhaltensweisen, womit legitime Aktivitäten von Journalisten, Whistleblowern, Sicherheitsforschern und anderen kriminalisier werden.

Es kann schwerwiegende Folgen haben, wenn den Menschenrechten nicht in allen Kapiteln Priorität eingeräumt wird. Der Schutz der Grundrechte wurde von Mitgliedstaaten während der Sitzungen des Ad-hoc-Ausschusses zur Ausarbeitung des Übereinkommensvorschlags immer wieder thematisiert. Viele Staaten und nichtstaatliche Interessengruppen forderten, dass das vorgeschlagene Übereinkommen umfassend mit den internationalen Menschenrechten in Einklang stehen muss. Sämtliche vorgesehenen Maßnahmen zur Einschränkung von Rechten müssen gesetzlich fixiert werden und bedürfen einer rechtlichen legitimierenden Begründung, die Bezug auf die betreffenden Rechte nimmt, und womit ein legitimes Ziel in erforderlicher und verhältnismäßiger Weise verfolgt wird. Die Bestimmungen müssen Rechtsstaatlichkeit respektieren durch ausreichende Spezifizierungen und die Sicherstellung einer und unabhängige Aufsicht, deren Umsetzung im beabsichtigten Rahmen bleibt.

Es ist äußerst beunruhigend, dass viele Bestimmungen des CND so formuliert sind, dass sie die Menschenrechte weder inhaltlich noch prozedural wahren, so dass für weitere Verletzungen der Menschenrechte und der Rechtsstaatlichkeit bei der Umsetzung Tür und Tor geöffnet werden.

Uns beunruhigt insbesondere, dass die Kataloge 2 bis 10 eine lange Liste von Straftaten enthalten, die keine typische Cyberkriminalität sind, sowie Straftatbestände, die den Schutz der Meinungsäußerung beeinträchtigen und die zulässigen Einschränkungen gemäß den internationalen Standards für die Meinungsfreiheit ignorieren oder die mit vage und extensiv formuliert sind.

Das Kapitel über Strafverfolgung sollte auf Kernkriminalität im Internet beschränkt werden, also auf Straftaten, bei denen Systeme der Informations- und Kommunikationstechnologie (IKT) sowohl direktes Ziel oder Instrument der Taten sind, Verbrechen, die ohne IKT überhaupt nicht möglich wären. Eine nützliche Referenz für die Arten von Straftaten, die von Natur aus IKT-Straftaten sind, findet sich in den Artikeln 2-6 der Budapester Konvention. Sollten andere Cyberkriminalität einbezogen werden, empfehlen wir, diese „cybergestützten“ Straftaten eng und strikt im Einklang mit internationalen Menschenrechtsstandards zu definieren.

Straftatbestände, bei denen IKT-Systeme einfach ein Werkzeug sind, das manchmal bei der Begehung verwendet wird, sollten von dem vorgeschlagenen Übereinkommen ausgenommen werden. Dazu gehören solche Tatbestände, die nach geltendem innerstaatlichem Recht verboten sind und nur zufällig IKT-Systeme betreffen oder die solche Systeme nutzen, ohne sie Systeme anzugreifen oder zu schädigen, was bei einigen der Tatbestände in den Katalogen 2 und 10 der Fall ist.

Wir sind besonders besorgt über die Aufnahme von Inhaltsdelikten wie „Straftaten im Zusammenhang mit Extremismus“ (Artikel 27) und „Straftaten im Zusammenhang mit Terrorismus“ (Artikel 29). Diese Bestimmungen missachten bestehende Menschenrechtsstandards, wie sie von verschiedenen UN-Gremien zu Richtlinien und nationalen Strategien zur Bekämpfung und Prävention von Terrorismus und gewaltbereitem Extremismus präzisiert wurden. Insbesondere Vertreter von Organisationen zur Meinungsfreiheit haben bekräftigt, dass weit gefasste und undefinierte Begriffe wie „Terrorismus“ und „Extremismus“ nicht zur Grundlage zur die Einschränkung der Meinungsfreiheit verwendet werden sollten. Es gibt zudem keine einheitlichen Definitionen dieser Konzepte im Völkerrecht, viele Staaten nutzen diese Mehrdeutigkeit, um unter anderem Menschenrechtsverletzungen wie politisch motivierte Verhaftungen und strafrechtliche Verfolgung von Mitgliedern der Zivilgesellschaft, unabhängigen Medien und Oppositionsparteien zu rechtfertigen.

Allgemeiner gesagt: Die Einbeziehung mehrerer inhaltsbezogener Straftaten ist zutiefst besorgniserregend (z.B. Straftaten in den Katalogen 4, 7, 8 und 9). Wie wir immer wieder während der Verhandlungen gefordert haben, sollte diese Konvention keine Äußerungsdelikte enthalten. Die Einbeziehung dieser Tatbestände birgt ein erhöhtes Risiko, dass die vorgeschlagene Konvention gegen den bestehenden internationalen Schutz der Meinungsfreiheit verstößt und dazu verwendet wird, die geschützte Meinungsäußerung nach internationalen Menschenrechtsstandards einzuschränken.

Darüber würden Maßnahmen gegen in Katalog 1 aufgeführten Kerndelikte der Cyberkriminalität zu Einschränkungen zu wesentlichen Arbeitsmethoden von Journalisten, Whistleblowern und Sicherheitsforschern führen, weshalb diese überarbeitet werden müssen. Artikel 6 und 10 beispielsweise sollten sich auf betrügerische Absichten und auf Schadenswirkungen beschränken –was viele Delegationen während der Diskussion zu diesem Thema auf der zweiten Fachtagung als dringend zu berücksichtigen gefordert haben.

Auch die Bestimmungen zu den Verfahrensbefugnissen in der Konvention geben Anlass zur Sorge. Die von der Konvention geforderten Ermittlungsbefugnisse sollten nur in Bezug auf Straftaten zur Verfügung stehen, die unter die Konvention fallen. Das Übereinkommen betrifft die Cyberkriminalität und darf nicht zu einem Allzweckinstrument zur Untersuchung jedweder Straftat werden.

Die allgemeine Verpflichtung zur Achtung der Grundsätze der Verhältnismäßigkeit, Erforderlichkeit und Rechtmäßigkeit sowie des Schutzes der Privatsphäre und personenbezogener Daten bei der Umsetzung von Verfahrensbefugnissen sind zu begrüßen; es sind aber zusätzliche Sicherungen zur Achtung der Menschenrechte bei der Umsetzung des Übereinkommens erforderlich. Zu diesem Zweck sollte Artikel 42 eine vorherige unabhängige (vorzugsweise gerichtliche) Genehmigung und eine unabhängige Ex-post-Überwachung vorsehen, die Notwendigkeit wirksamer Rechtsbehelfe anerkennen, eine strenge Transparenzberichterstattung und Benutzerbenachrichtigung durch die Vertragsstaaten fordern und Garantien vorsehen, dass Untersuchungsbefugnisse nicht die Integrität und Sicherheit digitaler Kommunikation und Dienste beeinträchtigen.

Die Verfahrensmechanismen der Konvention sollten zudem sicherstellen, dass internationales Recht und Menschenrechtsstandards in Bezug auf Beweismittel eingehalten werden. Beweise, die unter Verstoß gegen innerstaatliches Recht oder Menschenrechte erlangt wurden, sollten von Strafverfahren ausgeschlossen werden, ebenso wie alle weiteren Ergebnisse aus diesen Beweisen.

Die Sicherungsbefugnisse des Übereinkommens (Artikel 43 und 44) sollten gewährleisten, dass Aufbewahrungspflichten und Verlängerungen die begründete Annahme oder den Verdacht voraussetzen, dass eine Straftat begangen wurde oder begangen wird, und dass die Daten, deren Aufbewahrung beantragt wird, Beweise für diese Straftat liefern werden. Der Aufbewahrungszeitraum sollte, mit Verlängerungsmöglichkeit, sechzig (60) Tage nicht überschreiten; das Übereinkommen sollte klarstellen, dass nationale Gesetze keine Aufbewahrung über den angegebenen Zeitraum hinaus zulassen dürfen. Artikel 43 sollte zudem präzisieren, dass Diensteanbieter verpflichtet sind, alle aufbewahrten Daten unverzüglich zu löschen, sobald der Aufbewahrungszeitraum abgelaufen ist.

Artikel 46 Absatz 4 begründet ernsthafte Bedenken in Bezug auf mögliche

Verpflichtungen für Dritte wie z.B. Diensteanbieter, entweder Schwachstellen bestimmter Software offenzulegen oder den zuständigen Behörden Zugang zu verschlüsselter Kommunikation zu gewähren.

Artikel 47 zur Erfassung von Verkehrsdaten in Echtzeit sollte überarbeitet und präzisiert werden, um sicherzustellen, dass der Artikel keine pauschalen oder willkürlichen Maßnahmen zur Vorratsdatenspeicherung zulässt. Es ist davon auszugehen, dass das allgemeine Abfangen, Speichern oder Aufbewahren von Kommunikationsinhalten oder der Metadaten die Verhältnismäßigkeitsprüfung nicht besteht.

Die Artikel 47 und 48 sollten zur Klarstellung geändert werden, dass das staatliche Hacken von Endgeräten nicht erlaubt ist. Staatliche Hacking-Befugnisse sind nach wie vor umstritten und können die Integrität und Sicherheit von Netzwerken, Daten und Geräten kollektiv schädigen. Es besteht kein Konsens darüber, wann diese Befugnisse angemessen geltend gemacht werden können; es besteht die Gefahr, dass einige Vertragsstaaten die Artikel 47 und 48 unangemessen umsetzen, um diese Art der eingreifenden Überwachung einzubeziehen.

Die Vertraulichkeitsbestimmungen des Übereinkommens (Artikel 43 Abs. 3, 47 Abs. 3 und 48 Abs. 3) sollten darauf beschränkt werden, dass sie zur Verhinderung jeglicher Gefährdung von Ermittlungen erforderlich sind, die sich aus dem Fehlen der Vertraulichkeit ergeben könnten.

Bei allem Respekt empfehlen wir die Überarbeitung der CND, um Folgendes sicherzustellen:

- Der Anwendungsbereich des Übereinkommens sollte auf Angelegenheiten im Bereich des Strafjustizsystems beschränkt sein und sowohl in seinem sachlichen als auch in seinem verfahrensrechtlichen Anwendungsbereich auf Kernkriminalität im Internet beschränkt sein.
- Die vorgeschlagenen Straftaten gemäß den Artikeln 6 und 10 sollten im Interesse des Schutzes von Journalisten, Informanten und Sicherheitsforschern so überarbeitet werden, dass sie sich auf betrügerische Absicht auf Schadenswirkungen beschränken zu schützen [Katalog 1].
- Die Kapitel zu den Straftatbeständen sollten auf Taten gegen die Vertraulichkeit, Integrität und Verfügbarkeit von Computerdaten und -systemen beschränken.
- Straftaten, bei denen IKT lediglich ein Werkzeug ist, das manchmal bei der Begehung einer Straftat eingesetzt wird, sollten von dem Übereinkommen ausgenommen werden [Kataloge 2–10].
- Sollen andere Delikte aufgenommen werden, die nicht zum Kerngeschäft der Cyberkriminalität gehören, empfehlen wir eine eingrenzende und mit internationalen Menschenrechtsstandards zu vereinbarende Definition ist; in keinen Fall sollten Äußerungsdelikte aufgenommen werden.
- Straftatbestände, die Aktivitäten in einer Weise einschränken, die mit den Menschenrechten nicht vereinbar ist, sollten ausgeschlossen werden. Die Gefahr, dass über eine übermäßige Liste von Delikten zu Online-Inhalten, Sprachäußerungen und anderen Ausdrucksformen diese als Cyberkriminalität im Sinne des vorgeschlagenen Übereinkommens werden können, ist ein großes Problem, das durch die Entfernung von Äußerungsdelikten angegangen werden sollte [Siehe Katalog 4, 7, 8 und 9].
- Ermittlungsbefugnisse in Kapitel III zu strafprozessualen Maßnahmen und Strafverfolgung sollten sorgfältig abgegrenzt werden, damit sie eng an Ermittlungen zu bestimmten kriminellen Handlungen und Verfahren gebunden bleiben und nur für Ermittlungen zu Straftaten zur Verfügung stehen, die ausdrücklich unter das Übereinkommen fallen (Artikel 41 Absatz 2).
- Geheimhaltungsbestimmungen sollten nur gelten, wenn die Offenlegung der fraglichen Informationen eine nachweisbare Bedrohung für eine einschlägige Untersuchung darstellen würde (Artikel 43 Abs. 3, 47 Abs. 3 und 48 Abs. 3).
- Bei strafprozessualen Maßnahmen sollten Vorkehrungen bei den Ermittlungen und bei der Strafverfolgung vorgesehen werden, die detaillierte und solide Menschenrechtsgarantien und rechtsstaatlichen Standards mit sich bringen, einschließlich der Forderung nach unabhängiger Aufsicht und Kontrolle und dem Recht auf einen wirksamen Rechtsbehelf.
- Die allgemeinen Bestimmungen, die das Abhören und Sammeln von Daten in Echtzeit zulassen, sollten dahingehend klarstellend geändert werden, dass sie kein Eindringen in Netzwerke und Endgeräte zulassen. Es fehlen bisher ausreichende Garantien, um der Bedrohung der Sicherheit und Integrität von Netzwerken, Daten und Geräten durch staatliches Hacking zu begegnen; die Vertragsstaaten sollten sich nicht auf Mehrdeutigkeiten im Text berufen können, um Hacking-Aktivitäten zu rechtfertigen (Artikel 47 und 48).
- Der Text sollte keine willkürliche oder unbefristete Aufbewahrung von Metadaten erlauben.

Das Aushandeln eines internationalen Übereinkommens über Cyberkriminalität ist keine leichte Aufgabe. Es ist jedoch von größter Bedeutung, dass diese Konvention, die das Potenzial hat, Millionen von Menschen auf der ganzen Welt massiv zu beeinflussen, eindeutig klarstellt, dass die Bekämpfung der globalen Cyberkriminalität die Menschenrechte stärken und nicht gefährden oder untergraben sollte.

Vorgelegt von zivilgesellschaftlichen und akademischen Unterzeichnenden, die sich für die Teilnahme an den Sitzungen des Ad-hoc-Ausschusses zur Ausarbeitung eines umfassenden internationalen Übereinkommens zur Bekämpfung der Nutzung von Informations- und Kommunikationstechnologien für kriminelle Zwecke gemäß Operativ Nr. 8 oder Nr. 9 angemeldet haben.

Access Now – International; ARTICLE 19 – International; Association for Progressive Communications (APC) – International; Data Privacy Brasil – Brazil; Derechos Digitales - Latin America; Electronic Frontier Foundation – International; Eticas Data Society Foundation – International; Global Partners Digital – International; Human Rights Watch – International; Privacy International – International; Red en Defensa de los Derechos Digitales - Mexico u.v.a.m.

Der englischsprachige Originaltext des Offenen Briefs findet sich im Internet unter https://www.crime-research.org/news/10.01.2023/4112/.

Aufruf an Mitglieder des LIBE-Ausschusses

Cybercrime-Bekämpfung spielt auf vielen internationalen Ebenen derzeit eine wichtige Rolle. Im Rahmen einer abgestimmten Kampagne mehrerer NGOs hat die DVD Mails an alle Mitglieder des LIBE-Ausschusses des EU-Parlaments mit einem Aufruf zur Abstimmung zu einem Abkommen, das vom Europarat (nicht zu verwechseln mit dem Rat der Europäischen Union) vorgeschlagen wurde, versandt, welchen wir hier auch abdrucken:

Dear MEP,

I am writing on behalf of Deutsche Vereinigung für Datenschutz e.V. (DVD).

On Thursday 12 January you will vote on the draft recommendation on the draft Council decision authorising Member States to ratify, in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (06438/2022 – C9 0146/2022 – 2021/0383(NLE)).

However, this Second Additional Protocol is likely incompatible with the EU Treaties including the Charter of Fundamental Rights. We therefore ask you to not give consent to its ratification by supporting and vote in favour of the draft recommendation put forward by the Rapporteur.

We strongly believe that the European Parliament should not give its consent to the ratification of the Second Additional Protocol to the Convention on Cybercrime (hereafter 'the Protocol') for the following reasons:

1. The Protocol has several important shortcomings in terms of data protection and procedural rights, which makes it unlikely to be compatible with EU's high data protection and privacy standards. EDRi's analysis shows that, if ratified by the EU Member States without further amendments, the Protocol could lead to substantive breaches of EU law.

2. As an international agreement, the Protocol takes precedence over EU secondary law, which includes the General Data Protection Regulation (GDPR) and the Law Enforcement Directive (LED), and hence, may undermine important safeguards in these instruments.

3. Civil society, lawyers organisations and EU institutions, among others EDRi, the European Data Protection Board (https://edpb.europa.eu/our-work-tools/our-documents/other/edpb-contribution-6th-round-consultations-draft-second_en), the EU Fundamental Rights Agency (https://rm.coe.int/0900001680a2588f), the Council of Bars and Law Societies of Europe (CCBE) (https://rm.coe.int/0900001680a25786) and Access Now (https://rm.coe.int/0900001680a25783), have been continuously calling for stronger protections of fundamental rights in the Protocol negotiations. However, the modifications and improvements were not incorporated into the final text. Likewise, the draft Council Decision leaves too much discretion to Member States whether or not to implement stronger protections which might lead to different protection standards inside the EU, including regarding the right to an effective remedy and to a fair trial.

4. Preventing Member States from acceding to the Protocol is all the more important that there are 66 Parties to the Convention today, including the United States of America and other countries beyond Council of Europe members that do not have comprehensive data protection laws in place in their countries. Any State may accede to the Convention upon invitation in the future. The Protocol allows transfers of personal data directly from private service providers in the EU to law enforcement authorities in any current or future Party to the Protocol.

5. If the Protocol is found to be incompatible with the EU Treaties in the coming years, this would inevitably create serious legal difficulties for the EU internally and for the EU's international cooperation with third countries.

6. The Protocol's "breaks system" is severely lacking: the powers of the EU independent Data Protection Authorities (DPAs) to suspend transfers to States that are suspected of being in breach of their data protection obligations are severely constrained by the Protocol. DPAs cannot act independently, as required by EU primary law, in this regard.

In light of the above, we encourage you to support the Rapporteur's draft recommendation.

We thank you for your consideration and invite you to reach out to us should you have any questions.

On behalf of the board of DVD,

Mit freundlichen Grüßen / Best Regards
Frank Spaeing, Vorsitzender
Deutsche Vereinigung für Datenschutz e.V.

Digitale Identität: Offener Brief zur eIDAS-Reform an das Europäische Parlament (1. Februar 2023)

(Dear President and Vice Presidents MEP Metsola, MEP Karas, MEP Picierno, MEP Pereira, MEP Kopacz, MEP Regner, MEP Wieland, MEP Barley, MEP Charanzová, MEP Šimečka, MEP Beer, MEP Zīle, MEP Papadimoulis, MEP Hautala, Dear Rapporteur, Opinion Rapporteurs and Shadow Rapporteurs MEP Jerković, MEP Terheş, MEP Arimont, MEP Ansip, MEP Terras, MEP Mituța, MEP Peksa, MEP Borchia, MEP Roos, MEP Kountoura, MEP Bielan, MEP Vandenkendelaere, MEP Pelletier, MEP Joron, MEP Maldonado López, MEP Maurel, MEP Benifei, MEP Breyer, MEP Melchior, MEP Kaljurand, MEP Toom, MEP Vilimsky, MEP Ernst)

Sehr geehrter Vorsitzender, sehr geehrte stellvertretende Vorsitzende und Abgeordnete,

die unterzeichnenden Organisationen der Zivilgesellschaft (NGOs), Wissenschaftler und Experten sind wegen den bevorstehenden Abstimmungen zur eIDAS-Verordnung (EU) 2021/0136 (COD) im Europäischen Parlament besorgt. Digitale Identitätssysteme haben weltweit große Bedenken hinsichtlich der Grundrechte aufgeworfen.

Die Organisationen der Zivilgesellschaft, die dieses Schreiben unterzeichnet haben, wollen die Europäische Union in die Pflicht nehmen die Grundrechte zu schützen und ein System zu schaffen, das die sensibelsten Gesundheits-, Finanz- und Identitätsdaten nicht an Dritte weitergibt. Wenn Europa in dieser wichtigen Frage führend sein will, müssen Sie dies richtig machen.

Wir erkennen den gut entwickelten Datenschutzrahmen und die Rechtsgrundlage an, die Basis der aktuellen Reform der digitalen Identität in Europa sind. Diese sind notwendige, aber nicht hinreichende Voraussetzungen für ein System, das sich als zentrale, allgegenwärtige Plattform eignet und von dem künftig der Zugang zu E-Government, Handel, Bildung, sozialen Diensten und dem Arbeitsmarkt abhängen kann.

Es ist von entscheidender Bedeutung, dass potenziell Nutzende eine echte Wahl haben, ob sie dieses System verwenden oder nicht. Daher ist es notwendig gesetzlich einen starken Diskriminierungsschutz für diejenigen Teile der Bevölkerung zu verankern, die sich entscheiden das neue digitale Identitätssystem nicht zu nutzen, oder die dies nicht nutzen können. Senioren, digital weniger versierte Bevölkerungsschichten und Menschen ohne Smartphone dürfen nicht allein durch das Fehlen einer digitalen Identität an ihrer gesellschaftlichen Teilhabe gehindert werden. Entsprechende Schutzmaßnahmen müssen sowohl für den öffentlichen als auch für den privaten Sektor bestehen. So werden nicht nur Grundrechtsverletzungen und die Verstärkung sozialer Ungerechtigkeiten vermieden; dies trägt auch dazu bei das notwendige Vertrauen in der Bevölkerung für den Erfolg eines Systems zu schaffen, das für die meisten Nutzer ein Instrument einer echten Wahl darstellt.

Folglich erwarten wir, dass ein von der EU geschaffenes digitales Identitätssystem den Prinzipien von Privacy by Design und by Default folgt. Es sollte technisch für die Betreiber des Systems, die verbundenen Unternehmen oder die Anbieter von Attributen unmöglich sein Kenntnis zu erlangen, wie Benutzer das System verwenden. Wenn das System große Verbreitung findet, könnte es einen panoptischen Überblick über alle Aspekte des täglichen Lebens liefern. Nur mit starken technischen Schutzmaßnahmen auf Architekturebene kann verhindert werden, dass Daten über das Benutzerverhalten kopiert und missbraucht werden können. Entsprechendes gelang bei dem digitalen EU-COVID-Zertifikat (EU) 2021/953 und ein solcher Standard muss auch hier eingehalten werden.

Privacy by Design verbietet auch die Erstellung einer eindeutigen und dauerhaften Kennung, die immer wieder dafür genutzt werden kann das Benutzerverhalten über Interaktionen mit einzelnen Unternehmen oder Regierungsbehörden hinweg zu verfolgen. Die Europäische Union wäre blauäugig zu glauben, dass eine eindeutige und dauerhafte Kennung nicht von Big-Tech-Unternehmen missbraucht würde, um deren Benutzer zu verfolgen und zu überwachen. Ein solches „Super-Cookie" würde nicht nur in mehreren Mitgliedstaaten ernsthafte verfassungsrechtliche Bedenken hervorrufen, sondern könnte auch den Zweck dieser Verordnung, datenschutzfreundliche Alternativen zu den dominierenden Big-Tech-Unternehmen zu bieten, zunichte machen. Letztendlich wird das System anhand der Robustheit und Wirksamkeit seiner technischen und rechtlichen Schutzmaßnahmen gegen die Überwachung und Profilerstellung von Benutzern beurteilt werden.

Deswegen muss die eIDAS-Verordnung regeln, welche Unternehmen oder staatlichen Stellen (Verwender) die Nutzer um welche Informationen bitten dürfen. Ein System, das den Zugriff auf Identitäts-, Finanz- und Gesundheitsinformationen von Hunderten von Millionen Menschen ermöglicht, wird immer eine lukrative Angriffsfläche für bösartige Akteure sein. Es muss in jedem Fall in jedem Mitgliedsstaat wirksame Rechtsschutzmöglichkeiten geben für Verbraucherschutz- und Betrugsbeschwerden im jeweiligen Hoheitsgebiet, unabhängig davon, wo der Verwender seinen Sitz hat. Eine wirklich vertrauenswürdige Umgebung kann nur entstehen, wenn Verwender von ihrem Niederlassungsmitgliedstaat für ihre Anwendung freigeschaltet werden müssen, bevor ihnen erlaubt wird persönliche Informationen von Benutzern über das neue System anzufordern. Dieser Aspekt wurde während der französischen Ratspräsidentschaft im Rat der Europäischen Union thematisiert. Zudem sollten staatlich zertifizierte Identifikationsdaten nur für Anwendungen verfügbar sein, wenn diese auf einer gesetzlichen Know-your-Customer-Verpflichtung beruhen.

Schließlich möchten wir das IT-Sicherheitsrisiko hervorheben, das durch die Verpflichtung zur Unterstützung qualifizierter Website-Authentifizierungszertifikate (QWACs) von Webbrowsern entsteht.[i] Obwohl dies kein direktes Problem der digitalen Identität ist, untergräbt es die Sicherheitsarchitektur des Internets auf Grund fragwürdiger kommerzieller Motive von Vertrauensdiensteanbietern. Dieser Ansatz hat in der Vergangenheit nicht nur dazu beigetragen die Sicherheit nicht zu erhöhen, da er den Nutzern verwirrende Informationen lieferte, sondern er ermöglicht auch die staatliche Überwachung des Internetverkehrs in großem Umfang[ii]. Letztendlich sind solche Maßnahmen der Sicherheit aller Benutzer abträglich und gefährden die Akzeptanz der Bevölkerung für den Vorschlag insgesamt.

Die diesen Brief unterzeichnenden Organisationen glauben, dass ein europäisches System, das Grundrechte respektiert, ein globaler Gamechanger sein kann. Wir bitten Sie dringend diese Punkte bei den bevorstehenden Abstimmungen im Ausschuss für Industrie, Forschung und Energie und im Plenum sowie bei den bevorstehenden Trilog-Verhandlungen zu berücksichtigen. Bitte berücksichtigen Sie in dieser wichtigen Diskussion die Perspektive der Bürgerinnen und Bürger. Für weitere Konsultationen stehen wir zur Verfügung.

Zusammenfassend sind dies unsere wichtigsten Punkte:

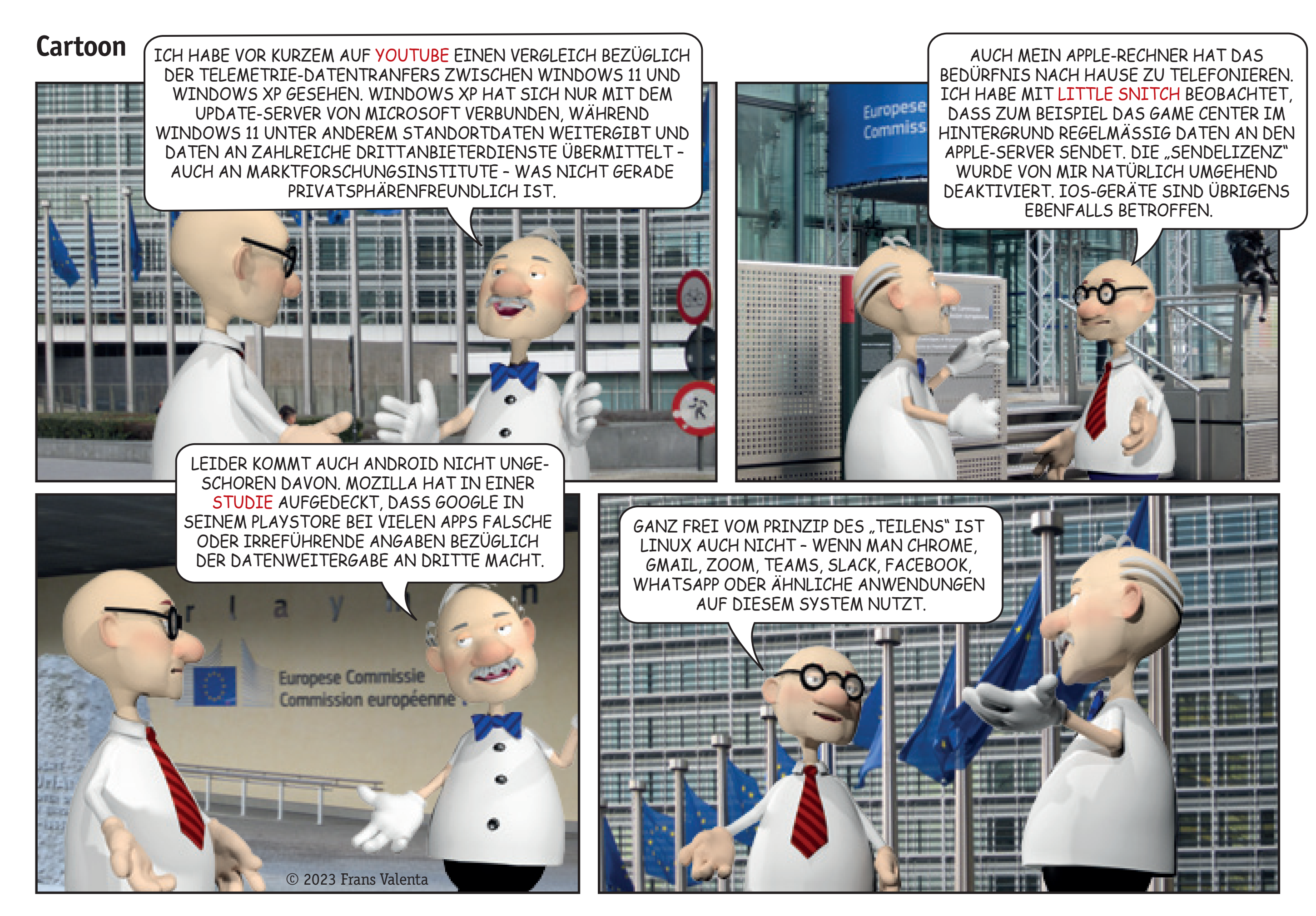
- Sicherung der freien Wahl über die Nutzung des digitalen Identitätssystems durch Schutzmaßnahmen vor Diskriminierung bei öffentlichen und privaten Dienstleistungen
- Verhinderung der Beobachtbarkeit des Benutzerverhaltens und aller persönlichen Transaktionen, die im System von Regierungen, Ausstellern und Attributanbietern vorgenommen werden
- Sicherstellung von Privacy-by-Design, indem keine eindeutigen und dauerhaften Kennungen festgelegt werden
- Effektive Regulierung von Anwendungsfällen, Verhinderung übermäßiger Informationsanfragen, Beschränkung von staatlich ausgestellten Identifizierungsinformationen auf solche, die auf einer gesetzlichen Know-your-Customer-Verpflichtung beruhen
- Verhinderung von Bestimmungen, welche die Unterstützung qualifizierter Website-Authentifizierungszertifikate von Webbrowsern vorschreiben.

Mit freundlichen Grüßen

Liste der Unterzeichnenden

(Der englischsprachige Originaltext ist im Internet abrufbar unter https://epicenter.works/document/4536, unsere deutsche Übersetzung (so wie hier abgedruckt) finden Sie unter https://www.datenschutzverein.de/wp-content/uploads/2023/02/eIDAS-Offener-Brief.pdf und hier finden Sie außerdem eine begleitende Informationsseite zum Thema: https://epicenter.works/content/die-europaeische-digitale-identitaet-ein-potenzieller-gamechanger.)

Cartoon



Datenschutznachrichten

Datenschutznachrichten aus Deutschland

Bund

Kelber kritisiert Verknüpfung von Steuer-ID mit IBAN

Laut Jahressteuergesetz soll die Steuer-ID mit Kontoverbindungsdaten zusammengeführt werden, um z.B. das Klimageld zahlen zu können. Es geht um die Frage, wie der Staat seinen Bürgern am einfachsten Geld wie die mit der Gas-, Wärme- und Strompreisbremse verknüpften Ausgleichszahlungen zukommen lassen kann. Der Gesetzgeber setzt dafür unter anderem darauf, dass das Bundeszentralamt für Steuern (BZSt) die umstrittene einheitliche Steuer-Identifikationsnummer bis 2024 mit der internationalen Kontonummer (IBAN) sowie gegebenenfalls dem BIC verknüpfen soll.

Der Bund der Steuerzahler macht Druck, das Vorhaben schleunigst in die Tat umzusetzen, so Daniela Karbe-Geßler, die bei der Interessenvertretung für Steuerpolitik zuständig ist: „Dies ist notwendig, um in Zukunft staatliche Leistungen, vergleichbar mit der Energiepreispauschale im September und Dezember des vergangenen Jahres, an die Bürger auszahlen zu können." Ohne diese Möglichkeit müssten andere Stellen den Ausgleich übernehmen, so wie 2022 die Rentenversicherung oder die Arbeitgeber. Die Lobbyorganisation moniert, dass das versprochene „Klimageld" bei vielen Empfangsberechtigten noch nicht auf dem Konto angekommen sei.

Der vom Bundestag Anfang Dezember mit dem Jahressteuergesetz 2022 beschlossene Ansatz stößt auf Kritik bei Datenschützern. Der Bundesdatenschutzbeauftragte Ulrich Kelber appellierte während des Gesetzgebungsverfahrens vergeblich an die Abgeordneten die Klausel zu überarbeiten und „verfassungsgemäße, mildere Mittel wie die Nutzung bereichsspezifischer Lösungen" oder den Rückgriff auf bereits vorhandene Datenbestände vorzusehen. Das Ziel, staatliche Direktzahlungen möglichst unkompliziert zu gestalten, sehe auch er zwar als „gesellschaftlich überragend wichtig an". Leider habe die Bundesregierung mit ihrem Entwurf dafür aber einen „datenschutzrechtlich nicht optimalen Weg gewählt".

Kelber monierte in einem Schreiben an den Finanzausschuss des Bundestags, dass bereits mit dem Registermodernisierungsgesetz die Steuer-ID zu einer Identifikations- und Bürgernummer für allgemeine Zwecke außerhalb der Finanzverwaltung geworden sei. Schon dies komme der Einführung eines bereichsübergreifenden Personenkennzeichens gleich, was das Bilden von Profilen „übermäßig" erleichtere und so „den besonders geschützten geistigen Innenraum" der Bürger gefährde. Es gebe keine hinreichenden Hürden, um Missbrauch effektiv zu verhindern. Die Weiterentwicklung der Steuer-ID zu einer nationalen Personen-Kennziffer war zwei Jahre zuvor von Datenschützern, Wissenschaftlern und Bürgerrechtlern kritisiert worden.

Gemäß Kelber wird diese an sich schon verfassungsrechtlich kritische Situation mit der Änderung im Jahressteuergesetz verschärft. Die dauerhafte Zusammenführung der Steuer-ID sowie der Identifikationsdaten gemäß der überarbeiteten Abgabenverordnung mit der zuletzt verwendeten IBAN beim BZSt „erhöht deren Erfassbarkeit durch eine neugewonnene Verlässlichkeit bei der Zuordnung und Weiterverarbeitung, dies gepaart mit einer stark herabgesenkten Hemmschwelle zur Weiternutzung". Nach den Maßstäben der ständigen Rechtsprechung des Bundesverfassungsgerichts seit dem Volkszählungsurteil greife dies „massiv in das grundrechtlich abgesicherte Recht auf informationelle Selbstbestimmung ein". Die Grünen hatten 2021 noch moniert, dass die Frage der Verfassungskonformität aufgrund der Steuer-ID wie ein Damoklesschwert über der Registerumstellung hänge.

Derweil ist nicht absehbar, wann die Verknüpfung von IBAN und Steuer-ID wirklich kommt. Finanzminister Christian Lindner prognostizierte schon im Sommer 2022, das Direktauszahlungsprojekt könne „achtzehn Monate" brauchen. Ein Ministeriumssprecher meinte, es müsse noch viel Technisches und Administratives geklärt werden. Wirtschaftsminister Robert Habeck schätzt, dass es erst in der nächsten Legislaturperiode, die regulär im Herbst 2025 beginnt, Direktzahlungen geben werde. Die Digitalisierung der Verwaltung erfolgt weiterhin im Schneckentempo (Krempl, Datenschutz: Kritik an „Personenkennziffer" aus Kontonummer und Steuer-ID, www.heise.de 07.01.2023, Kurzlink: https://heise.de/-7451758, Prantl, 12345678910, SZ 14./15.01.2023, 5; Schloemann, Auf der Suche nach der Bürgernummer, SZ 31.01.2023, 5).

Bund

Erweiterter Zugriff auf SIS III

Am 01.12.2022 hat der Bundestag mit den Stimmen der Fraktionen der Ampel-Koalition und der CDU/CSU einen Gesetzentwurf verabschiedet, der Details zur Durchführung von drei EU-Verordnungen von 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der dritten Generation (SIS III) regelt. Die Linksfraktion stimmte gegen den Entwurf. Mit dem Gesetz sollen in Deutschland über 2.000 zusätzliche Behörden direkt an das europäische Sicherheits- und Fahndungssystem angeschlossen werden, das Ende 2021 knapp 90 Millionen Datensätze enthielt.

Bisher hatten ausschließlich berechtigte Mitarbeiter von Ämtern der Mitgliedstaaten aus den Bereichen Strafverfolgung und Justiz wie etwa Grenzschutz, Polizei, Zoll und Visa Zugriff auf die umfangreiche Datenbank. Dazu kamen einzelne Zulassungsstellen und EU-Behörden wie Europol. Nun kommen in Deutschland u.a. die Ausländerbehörden, das Auswärtige Amt, das Bundesamt für Auswärtige Angelegenheiten, die Auslandsvertretungen, das Bundesamt für Migration und Flüchtlinge (BAMF), die Wasserstraßen- und Schifffahrtsämter sowie das Luftfahrt-Bundesamt dazu. In den Verbund integriert werden zudem alle für die Kfz-Zulassung zuständigen Ämter, die Waffenbehörden, die Staatsanwaltschaften sowie die obersten Landesbehörden im Rahmen ihrer Zuständigkeiten nach dem Aufenthaltsgesetz.

Durch eine Änderung des Bundesverfassungsschutzgesetzes erhalten die deutschen Geheimdienste – das Bundesamt für Verfassungsschutz als Inlandsgeheimdienst, der Bundesnachrichtendienst (BND) und der Militärische Abschirmdienst (MAD) – die Befugnis über das Bundeskriminalamt (BKA) Ausschreibungen zur verdeckten Fahndung im SIS vornehmen zu lassen. Dies kann Personen wie Flüchtlinge oder Aktivisten, bargeldlose Zahlungsmittel oder andere Sachen betreffen. Bei einer solchen verdeckten Fahndung erfährt die ausschreibende Behörde etwa bei einer polizeilichen Verkehrskontrolle oder einem Grenzübertritt, wohin ein betroffenes Individuum wann und mit wem gereist ist. Ermittler können die entsprechenden Daten speichern und vor einem späteren möglichen Zugriff zunächst zu umfassenden Bewegungs- sowie Kontaktprofilen verdichten.

Von ihrer Kompetenz, Verdächtige über das SIS grenzüberschreitend heimlich zu überwachen, machten europäische Polizeibehörden schon in der Vergangenheit verstärkt Gebrauch. Das Blackbox-Verfahren dürfte mit der offiziellen Erlaubnis für Geheimdienste für solche Fahndungen nun noch viel öfter verwendet werden. Clara Bünger, Sprecherin für Flucht- und Rechtspolitik der Linksfraktion im Bundestag, meinte, die Befugnis verstoße gegen das verfassungsrechtliche Trennungsgebot zwischen Polizei und Geheimdiensten. Dadurch erhielten die Agenten nämlich „unmittelbar Zugriff auf die Befugnis der Polizei zur Personenkontrolle".

Im Hintergrund verknüpft die EU parallel seit 2019 sämtliche bestehenden und sich im Aufbau befindlichen EU-Datenbanken in den Bereichen Sicherheit, Grenzmanagement und Migrationssteuerung. Dazu kommt ein übergeordneter „Speicher für Identitätsdaten", eingeschränkt zunächst auf Angehörige von Drittstaaten. Unter dem Aufhänger „Interoperabilität" entsteht de facto eine umfassende Biometrie-Datenbank.

Der Bundesdatenschutzbeauftragte Ulrich Kelber äußerte sich kritisch zu dem Vorhaben: „Die Erweiterung einer Datenbank, sei es durch den Anschluss neuer Stellen, die Verarbeitung weiterer Datenkategorien oder die Verknüpfung mit anderen Systemen, birgt grundsätzlich ein erhöhtes Risiko für Fehler bei der Datenverarbeitung." Dies schließe missbräuchliche Nutzungen ein. Manuel Höferlin, innenpolitischer Sprecher der FDP-Fraktion, begrüßte, dass mit der neuen BKA-Zentralstellenfunktion für das SIS „schnelle europaweite Fahndungen" ermöglicht würden. Dabei werde der nationale Teil der Datenbank vom deutschen polizeilichen Informationsverbund Inpol technisch getrennt. Um die geplante und nötige Inbetriebnahme des SIS III zu gewährleisten, habe das Bundesinnenministerium bereits in den vergangenen Jahren die technischen Umsetzungsvoraussetzungen geschaffen. Die Entscheidungskompetenz rund um die nun erfolgten Gesetzesanpassungen hätten aber beim Parlament gelegen (Krempl, 2000 weitere Behörden erhalten Zugriff aufs Schengen-Informationssystem, www.heise.de 02.12.2022, Kurzlink: https://heise.de/-7365362).

Bund

EES und ETIAS werden national umgesetzt

Die Bundesregierung hat dem Bundestag einen Gesetzesentwurf für das europäische Ein- und Ausreisesystem („Entry/Exit-System" – EES) zur Biometrie-Grenzkontrolle sowie für das Europäische Reisegenehmigungssystem (ETIAS) vorgelegt. Sie möchte damit sicherstellen, dass die EU-Verordnungen zu EES und ETIAS in Deutschland reibungslos angewandt werden können. Die direkt in allen Mitgliedstaaten geltenden EU-Vorgaben müssen durch nationale Rechtsnormen wie z.B. das Aufenthaltsgesetz ergänzt werden. Dazu gehören auch die Festlegungen der innerdeutschen Zuständigkeiten für vorgesehene Aufgaben und technische Vorgaben.

Im EES mit biometrischer Grenzkontrolle müssen sich Bürger aus Drittstaaten künftig im Rahmen des „Smart Borders"-Programms mit vier Fingerabdrücken und biometrischem Gesichtsbild in der EU registrieren lassen. Die Datenbank soll „intelligente Grenzkontrollen" nach US-Vorbild ermöglichen, die zulässige Dauer eines Kurzaufenthalts berechnen und bei Überziehung automatisch die nationalen Sicherheitsbehörden verständigen.

Visumsfrei in die Gemeinschaft einreisende Personen sollen mithilfe von ETIAS vorab durchleuchtet werden. Sie müssen über einen Online-Antrag den Behörden persönliche Informationen u.a. zu Identität, Reisedokument, Aufenthaltsort, Kontaktmöglichkeiten, infektiösen Krankheiten und Ausbildung mitteilen. Die Daten sollen dann automatisch mit Daten aus zahlreichen anderen europäischen IT-Systemen, einer virtuellen Biometrie-Superdatenbank sowie Registern von Interpol abgeglichen und gespeichert werden. Pate gestanden hat das 2007 von den USA entwickelte Einreisegenehmigungssystem ESTA. Ziel ist festzustellen, ob eine Einreise in den Schengenraum grundsätzlich berechtigt ist, und ob damit ein Risiko für Sicherheit, geregelte Migration oder Gesundheit verbunden sein könnte.

Für die EES-Übermittlungsvorgänge plant die Regierung ein automatisiertes Verfahren, für dessen technische Umsetzung sie anderthalb Jahre veranschlagt. Bis dahin sollen Meldungen zwischen rund 224 Auslandsvertretungen und weiteren Behörden gemäß der Gesetzesbegründung „vermutlich als PDF-Datei per E-Mail" erfolgen. Eine Pflicht zur Verschlüsselung der erwarteten rund 37.500 Notizen wird nicht

angesprochen. Das Sicherheits- und Qualitätsniveau vor allem des EES soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) überprüfen. Dazu kann es dem Plan nach zur „Unterstützung bei der Bewältigung von Sicherheitsvorfällen" auf Anfrage Einzeldaten von der Bundespolizei und dem Bundesverwaltungsamt erhalten. Insbesondere bei elektronischen Fälschungen von Reisepässen seien nur so forensische Analysen des Chips für das BSI möglich. Diese wiederum hülfen technische Sperrlisten zu aktualisieren oder die Richtlinie zur technischen Dokumentenprüfung fortzuschreiben. Die Gesetzesvorlage rechnet auch mit Sicherheitsproblemen durch neue Angriffsvektoren wie elastische 3D-Drucker-Masken und 3D-Schminken oder lokale Fehlkonfigurationen der Biometrie-Algorithmen („Schwellwertfehler"). Eine „Presentation Attack Detection" soll den Einsatz von Spezialmasken verhindern. Solche Gegenmaßnahmen können gemäß dem Entwurf nur auf Basis der im Einzelfall zu übermittelnden Daten optimiert werden. Dies gelte auch für den Bereich von Vorkommnissen durch „Morphing, also dem Fusionieren von mehreren Bildern zu einem einzigen zur Nutzung eines Passes durch mehrere Personen" (Krempl, EU-Datenbanken: Bund will biometrische Grenzüberwachung ausweiten, www.heise.de 24.01.2023, Kurzlink: https://heise.de/-7469954).

Bundesweit

Verhaltensregeln für Auftragsverarbeiter genehmigt

Auf der Datenschutz-Fachkonferenz DAFTA in Köln wurden am 17.11.2022 die „Trusted Data Processors" vorgestellt, mit denen sich Auftragsverarbeiter über frisch genehmigte Verhaltensregeln (Codes of Conduct) zertifizieren können. Damit soll die Anwendung der Datenschutz-Grundverordnung (DS-GVO) in der Praxis insbesondere für kleine und mittelständische Unternehmen vereinfacht werden.

Niels Lepperhoff, Geschäftsführer der DSZ GmbH (DSZ), berichtete, dass er zusammen mit dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. und der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) insgesamt sechs Jahre an dem äußerst komplexen und aufwändigen Projekt gearbeitet habe, bevor die baden-württembergische Aufsichtsbehörde das Verfahren offiziell genehmigte. Derzeit seien auch andere Codes of Conduct in Arbeit, die unter anderem die korrekte Pseudonymisierung und Anonymisierung von Daten garantieren sollen.

Die vorgestellte Selbstverpflichtung soll den bisher notwendigen Aufwand wesentlich reduzieren, mit dem Auftraggeber sicherstellen, dass ihre Auftragnehmer die datenschutzrechtlichen Regelungen komplett erfüllen. Lepperhoff erläuterte, dass Dienstleister immer wieder Fragenkataloge von Kunden mit zum Teil mehreren hundert Fragen beantworten müssten, was in Zukunft massiv vereinfacht werden soll.

Anders als bei anderen Industriestandards – wie zum Beispiel dem Transparency and Consent Framework (TCF) – wurde hier von Beginn an Wert darauf gelegt, dass die Einhaltung der Regeln regelmäßig überprüft wird. Als Überwachungsstelle fungiert das Bonner Unternehmen DSZ. Wer gegen die Verhaltensregel verstößt, dem kann der Status als „Trusted Data Processor" wieder entzogen werden. Bußgelder können aber weiterhin nur die amtlichen Aufsichtsbehörden verhängen. Wer kein offizielles Siegel will, soll die Maßgaben auf der Webseite https://www.verhaltensregel.eu/ finden.

Der damalige baden-württembergische Datenschutzbeauftragte Stefan Brink meinte: „Selbstregulierung ist eine hervorragende Möglichkeit Datenverarbeitung maßgenau auf die Bedürfnisse von Branchen abzustimmen – die DSGVO gibt diese Möglichkeit, die wir jetzt umsetzen." Dieser Einstieg in die Selbstregulierung geht einher mit einer veränderten Aufgabenstellung der betrieblichen und behördlichen Datenschutzbeauftragten: Sie sollen künftig mehr als Datenmanager und nicht mehr als Bremser von Datenverarbeitungen fungieren (Kleinz, „Trusted Data Processor" – Einstieg in die DS-GVO-Selbstregulierung, www.heise.de 18.11.2022, Kurzlink: https://heise.de/-7345987).

Bundesweit

Durchsuchungen bei Google-Fonts-Abmahnern

Wegen des Verdachts auf Abmahnbetrug und Erpressungsversuch in mindestens 2.418 Fällen wurden in einem Verfahren gegen den 53-jährigen Anwalt Lenard aus Berlin und dessen 41-jährigen Mandanten Ismail – einem Vertreter einer ominösen „Interessengemeinschaft Datenschutz" – in Berlin, Hannover, Ratzeburg und Baden-Baden Durchsuchungsbeschlüsse und zwei Arrestbeschlüsse mit einer Gesamtsumme von 346.000 Euro vollstreckt. Im Nachgang der Durchsuchungen am 21.12.2022 werden laut der Staatsanwaltschaft in Berlin Unterlagen und Datenträger ausgewertet, die Aufschluss „über die Anzahl, Auswahlkriterien und Identität, die tatsächlichen Umsätze und die genaue Vorgehensweise" geben sollen.

Den Beschuldigten wird vorgeworfen, Privatpersonen und Kleingewerbetreibenden, die auf ihren Websites Google Fonts eingesetzt haben, mit einem Anwaltsschreiben abgemahnt zu haben. Zugleich wurde den Website-Betreibern angeboten ein Zivilverfahren gegen das Zahlen einer Vergleichssumme in Höhe von 170 Euro vermeiden zu können. Die Beschuldigten wussten allerdings, dass es keinen Anlass für eine derartige Vergleichssumme gegeben hat. Die Besuche der Websites wurden protokolliert, um die Betreiber abmahnen zu können. Doch der Anwalt und sein Mandat sollen, so der staatsanwaltliche Vorwurf, sie getäuscht haben, indem sie behaupteten, eine Person habe die Websites besucht. Da keine natürliche Person auf der Webseite gewesen sei, läge auch keine Verletzung eines Persönlichkeitsrechts vor. Zudem hätten sie diese Internetseiten bewusst besucht und dadurch faktisch der Datenübermittlung zugestimmt – womit es auch keinen Datenschutzverstoß gebe. In einigen Fällen seien auch gar keine Daten in die USA übermittelt worden.

Daher hätten die Forderungen gerichtlich nicht durchgesetzt werden können. Ca. 2.000 Personen hatten die Vergleichssumme gezahlt – zudem liegen 420 Anzeigen von Abgemahnten

vor, die der Zahlungsaufforderung nicht nachgekommen waren.

Mit einer selbst programmierten Software hatten die Beschuldigten die Websites ausgemacht, die Google Fonts nutzen und Websitebesuche anschließend getrackt und protokolliert. Die Besuche wurden dann als „Grundlage für die Behauptung der datenschutzrechtlichen Verstöße und die Geltendmachung von Schmerzensgeldansprüchen" genutzt und es wurden seit Sommer 2022 Abmahnungen verschickt. Die Beschuldigten hatten in vielen Fällen vorgegeben, dass eine Person auf der Website war, obwohl tatsächlich nur ein automatisierter Zugriff erfolgte. Außerdem hätten Personen vor einem Besuch der Seite einer Datenweitergabe zugestimmt, die Abmahnung erfolgte allerdings dennoch. Wirtschaftsverbände, Internetkenner und Juristen, u.a. auch die DVD, warnten vor der Abmahnmasche. Die Abmahner hatten die DVD sowie andere Organisationen zum Beleg ihrer Seriosität missbraucht, indem sie versuchten sich als Spender der gemeinnützigen Einrichtungen zu präsentieren (DANA 4/2022, 249).

MIt dem Fonts-Dienst stellt Google mehr als 1.400 Schriftarten zur kostenlosen Nutzung auf Webseiten zur Verfügung, ohne dass die Fonts auf eigenen Servern bereitgehalten werden müssen. Allerdings lädt der Besucher der Website die Fonts direkt von den Google-Servern und übermittelt dabei die IP-Adresse an Google – in der Regel ohne Kenntnis und Einwilligung der Webseitenbesucher. Das Landgericht (LG) München hatte am 20.01.2022 entschieden, dass die Weitergabe der Daten einen Verstoß gegen die Datenschutz-Grundverordnung (DSGVO) darstelle (Az. 3 O 17493/20). Dadurch habe der Kläger in diesem Fall einen Kontrollverlust über seine personenbezogenen Daten erlitten. Das Gericht sah eine immaterielle Verletzung des Klägers und gestand ihm Schadenersatz zu. Denn Google sei ein Unternehmen, das „bekanntermaßen Daten über seine Nutzer sammelt", befand das Gericht. Die Folge der rechtswidrigen Datenweitergabe sei ein „individuelles Unwohlsein", das so erheblich sei, dass es einen Schadenersatzanspruch rechtfertige. Das Urteil hatte sich das Duo Lenard und Ismail zunutze gemacht.

Fachleute kritisieren am LG-Urteil, das davon ausgeht, dass die Übermittlung der Daten in die USA „unstreitig" sei, es setze sich technisch wie rechtlich nicht hinreichend mit der Funktionsweise von Google Fonts auseinander. Es sollte in jedem Fall klar sein, dass auf entsprechende Forderungen nicht gezahlt werden sollte. Dringend zu empfehlen ist als Webseiten-Betreiber Google Fonts selbst zu hosten (Generalstaatsanwaltschaft Berlin, Gemeinsame Pressemeldung: Durchsuchungen nach Abmahnwelle wegen „Google Fonts"-Nutzung, 21.12.2022; Koch, Google-Fonts: Durchsuchungen wegen Abmahnungen vermeintlicher Datenschützer, www.heise.de 21.12.2022, Kurzlink: https://heise.de/-7440620; Fröhlich, Betrugsmasche „Google-Fonts": Razzia bei Berliner Abmahnanwalt Kilian Lenard, www.tagesspiegel.de 21.12.2022).

Baden-Württemberg/Bayern

Behörden untätig bei informationellem Tesla-Angriff?

Die DANA-Redaktion hat folgende Schilderung erhalten, die von Datenschutzinteresse ist, weil sie einerseits Hinweise darauf gibt, wie Tesla-Autos missbraucht werden können, zum anderen darauf, dass hier eine offensichtliche Persönlichkeitsverletzung durch Private durch behördliche Untätigkeit ignoriert wird:

„Mit dem Vermieter befand ich mich seit 2019 wegen dessen Eigenbedarfskündigung des von meiner Familie und mir bewohnten Wohnobjekts in einer juristischen Auseinandersetzung. Erkennbar ab […] 2021 stand der Vermieter häufig in unmittelbarer Nähe zum Eingang bzw. an der Zufahrt zur zugehörigen Garage mit seinem geparkten Tesla. Aus diesem Fahrzeug heraus wurden wir von ihm manchmal erkennbar mit dem Handy gefilmt. Weitaus öfter war das Fahrzeug jedoch dort abgestellt, ohne dass ein Fenster geöffnet war geschweige denn erkennbar sich Personen darin aufhielten. […]

Diese ständigen Überwachungen nahmen […] in steigender Intensität zu. Dies gipfelte […] darin, dass der Vermieter – nachdem er in seinem Tesla sitzend – […] stieg er aus dem Tesla aus, lief auf mich zu und blieb dann an der Fahrerseite stehen, wobei er die ganze Zeit mit dem Handy mich filmte. Gleichzeitig brüllte er herum, dass ich/wir auch sonst die ganze Zeit gefilmt würden. […]

Nachdem ich den Bericht im Fernsehen (über den Wächter-Modus bei Tesla-Fahrzeugen, die Redaktion) gesehen hatte, war mir klar, was er damit gemeint hatte: Nämlich den Einsatz der Tesla-Kameras, um meine Familie und mich, äußerlich nicht erkennbar, ständig zu filmen.

Aufgrund des Ereignisses am […] hatte ich bei der zuständigen Staatsanwaltschaft Anzeige u.a. wegen Nachstellung, Nötigung und Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen erstattet.

In dem eingangs erwähnten Fernsehbericht war erwähnt worden, dass das Bayrische Landesamt für Datenschutzaufsicht federführend für die bundesdeutschen Datenschutzaufsichtsbehörden bei der Überprüfung der Einhaltung der hiesigen datenschutzrechtlichen Regelungen bei der Datenverarbeitung bei Tesla-Fahrzeugen zuständig wäre.

Aus diesem Grund wandte ich mich – obwohl in Baden-Württemberg wohnend – erstmals im August 2021 an das Bayrische Landesamt für Datenschutzaufsicht und legte den gesamten Sachverhalt zur Prüfung vor. Parallel hatte ich auch einem Jahresbericht dieser Behörde entnommen, dass sie Präzedenz-Fälle suche, mit deren Hilfe sie die missbräuchliche Verwendung der Tesla-Kameras konkret überprüfen und nachweisen könne. Ich ging daher davon aus, dass der von mir geschilderte Sachverhalt genau dieser Präzedenzfall sein könnte.

In der Zwischenzeit ist mehr als ein Jahr vergangen und außer einer automatisierten Eingangsbestätigung konnte ich bis heute keine Reaktion von Seiten des Bayrischen Landesamts für Datenschutzaufsicht verzeichnen. Mehrere Nachfragen per Telefon, per E-Mail und per Fax blieben unbeantwortet. Zuletzt habe ich mich per Einschreiben an den Präsidenten dieses Amts gewendet: Wiederum keine Reaktion.

Mittlerweile habe ich auch […] eine datenschutzrechtliche Beschwerde

beim Landesdatenschutzbeauftragten für Baden-Württemberg eingereicht: Ebenfalls keine Reaktion.

Mittlerweile hat auch die Staatsanwaltschaft (StA Mannheim und GStA Karlsruhe) das bzw. die Verfahren einfach eingestellt. Meine Hinweise auf die Ausstattung von Tesla-Fahrzeugen mit Kameras zur pausenlosen Rundumüberwachung der Fahrzeugumgebung wurde überhaupt nicht zur Kenntnis genommen."

Hinweis: Weitere Informationen zum Thema finden sich in DANA 3/2022, 180 f., 185, DANA 2/2021, 116, 130, 131, Weichert, DANA 4/2020, 227 ff., sowie „Datenverarbeitung und Datenschutz bei Tesla-Fahrzeugen" unter https://www.netzwerk-datenschutzexpertise.de/sites/default/files/gut_2020tesla.pdf).

Berlin

Messerstecher offenbar durch Tesla-Aufnahmen identifiziert

Am 31.10.2022 passierte ein schwerer Unfall auf der Bundesallee in Berlin-Wilmersdorf, bei dem ein Betonmischer eine 44-jährige Fahrradfahrerin überrollte und einklemmte. Die Radfahrerin wurde später in einer Klinik intensivmedizinisch behandelt und musste für hirntot erklärt werden. Der Unfall verursachte große öffentliche Aufmerksamkeit, weil Klima-Aktivisten der „Letzten Generation" die A100 blockiert hatten und dadurch ein Spezialfahrzeug der Feuerwehr zum Anheben schwerer Lasten im Stau stecken blieb. Die Radfahrerin konnte so auf anderem Weg nur verspätet aus ihrer Verklemmung befreit werden.

In diesem Zusammenhang gab es eine Messerattacke auf den Lkw-Fahrer. Als der nach dem Unfall ausstieg, um nach der Frau zu sehen, wurde er von einem Mann attackiert und niedergestochen, wobei der 64-Jährige schwere Verletzungen erlitt. Zwei Tage später identifizierte die Polizei den mutmaßlichen Täter der Messerattacke. Es soll sich dabei um einen 48-jährigen Obdachlosen handeln, der festgenommen und einem Untersuchungsrichter vorgeführt wurde. Nach Angaben der Berliner Polizei gibt es Hinweise auf eine psychische Erkrankung bei dem Mann. Für die Ermittlung des mutmaßlichen Täters hatten Polizeibeamte die Aufnahmen eines zufällig vorbeifahrenden Teslas herangezogen. Die Autokamera filmte demnach die Tat und half damit bei der Identifizierung des Verdächtigen (Unfall auf der Bundesallee: Radfahrerin ist hirntot, www.morgenpost.de 03.11.2022).

Niedersachsen

Beschwerdenbelastung für Datenschutzaufsicht auf hohem Niveau

Die Zahl der Beschwerden zu möglichen Datenschutzverletzungen ist im Jahr 2022 in Niedersachsen gegenüber dem Vorjahr leicht gesunken. Insgesamt 2.058 Beschwerden von betroffenen Bürgerinnen und Bürgern gingen 2022 bei der Landesbeauftragten für den Datenschutz (LfD), Barbara Thiel, ein. Das waren knapp 500 weniger als noch ein Jahr zuvor. 2019 gingen den Angaben zufolge insgesamt knapp 1.900 Beschwerden ein, 2018 noch rund 1.000. Häufige Gründe, weshalb sich Bürger an die Landesbeauftragte wandten, waren den Angaben zufolge Videoüberwachung des öffentlichen Raums, die Veröffentlichung von personenbezogenen Daten auf Social Media oder die Offenlegung von Daten an unbefugte Dritte.

Auch die Meldungen mutmaßlicher Datenschutzverletzungen gemäß Art. 33 DSGVO von Unternehmen oder Behörden gingen demnach ebenfalls zurück. 2022 waren es 1.149 Meldungen, ein Jahr zuvor noch 1.673. Als Ursache für den Rückgang in diesem Bereich nannte der Sprecher, dass Beschwerden zu Sicherheitslücken bei einer Software im vergangenen Jahr keine Rolle mehr gespielt hätten – 2021 waren dazu knapp 500 Meldungen eingegangen. Lässt man dies außen vor, ist die Zahl der übrigen Meldungen etwa auf demselben Niveau geblieben. Wer eine Beschwerde bei der Stelle einreichen möchte, kann dies über ein Online-Formular oder alternativ per Post, E-Mail oder Fax tun. Der Grund für die Beschwerde soll dabei so detailliert wie möglich beschrieben werden (DSGVO: Weniger Beschwerden über Datenschutzverletzungen in Niedersachsen, www.heise.de 14.01.2023, Kurzlink: https://heise.de/-7459290).

Nordrhein-Westfalen

Fortgesetzter Streit um Krankenhaus-Altakten

Die Verantwortlichen im ostwestfälischen Büren bei Paderborn beschäftigt schon seit Jahren eine gewaltige Menge von Patientenakten, die in einem verfallenden Gebäude einer Klinik, die vor mehr als einem Jahrzehnt aufgegeben wurde, abgelegt sind. Die Aktenberge sind inzwischen in einen „Sarkophag" aus Stahlgittern und Mauern eingeschlossen. Das Verwaltungsgericht (VG) Minden soll nun entscheiden, wer für die Kosten der Sicherung verantwortlich ist. Der Bürgermeister der 21.000-Einwohner-Stadt, Burkhard Schwuchow, hofft, dass mit dem Verfahren Bewegung in den Fall kommt. Der habe sich als „unendliche Geschichte" herausgestellt, die nicht zu Ende gehen wolle. Die Stadt habe großes Interesse daran, dass es auf der Liegenschaft eine Entwicklung gebe – „und dass dieser Missstand behoben wird".

Der Datenskandal hatte 2020 für Schlagzeilen gesorgt. Damals veröffentlichte der Youtuber „Ist-Marvin" ein Video und zeigte, wie er durch eine unverschlossene Tür in das verlassene Gebäude geht und die Akten findet. Die Klinik stand da schon seit mehr als zehn Jahren leer (DANA 3/2020, 190). Schwuchow: „Zu dem Zeitpunkt waren die Akten für jeden mit genug krimineller Energie frei zugänglich." Die Auseinandersetzung über die Verantwortung für die Akten war dann Gegenstand eines gerichtlichen Disputs: Am 15.10.2020 entschied das Oberverwaltungsgericht Hamburg in zweiter Instanz im vorläufigen Rechtsschutzverfahren, dass die MK-Kliniken AG mit Sitz in Hamburg, die frühere 100%-ige Eigentümerin der insolvent gegangenen MK-Kliniken GmbH, als letzte Krankenhausbetreiberin aus Datenschutzsicht für die lagernden Patientenakten nicht verantwortlich sei, da diese nicht „verarbeitet" würden (OVG HH 15.10.2020 – 5 BS 152/20, DuD 2020, 272 mit ablehnender Anm. Wei-

chert). Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit wollte – erfolglos – die MK-Kliniken zu einem datenschutzkonformen Umgang mit den Altakten verpflichten.

Für die örtliche Ordnungsbehörde war es so gemäß Bürgermeister Schwuchow das Gebot der Stunde den „störenden Zustand" zu beseitigen: Fenster und Luftschächte wurden verriegelt, Türen mit Stahlgittern verschweißt. Und es wurde ein Sicherheitsdienst engagiert, anfangs war er 24 Stunden vor Ort. Laut einer Sprecherin des Verwaltungsgerichts Minden gab es einen „Patientenaktentourismus" von Nachahmern des YouTubers. Schwuchow: „Die konnten alle aufgegriffen werden. Sonst wäre zum wiederholten Male massivst das Datenschutzgeheimnis verletzt worden."

Das Geld für die damaligen Maßnahmen – gut 13.500 Euro – und die laufenden Kosten für die Alarmanlage – gut 300 Euro pro Monat – wollte die Stadt von der Eigentümerin zurück. Doch die klagte dagegen, so die Sprecherin des VG Minden, wo der Fall verhandelt wird. Erster Prozesstag war am 14.12.2022, das Urteil erging am 06.01.2023.

Die letzte Klinikbetreibergesellschaft in diesem verzwickten Fall wurde im April 2010 insolvent. Sie ist – wie die Eigentümergesellschaft, die nun mit der Stadt vor Gericht streitet – eine hundertprozentige Tochter der MK-Kliniken AG, früher Marseille-Kliniken AG. Ein Sprecher der MK Kliniken AG hatte 2020 bei Presseanfragen auf den Insolvenzverwalter verwiesen, der für die ordnungsgemäße Entsorgung und Lagerung der Akten verantwortlich sei.

Schwuchow sagt, er glaube, dass es auch für die Betroffenen der „sicherlich weit über 1.000 Akten" gut sei, dass ein Gericht über das künftige Verfahren mit den Akten entscheide: „Wir gehen davon aus, dass sämtliche Akten seit Bestehen dieses Krankenhauses dort lagern." Es ist mehr als 150 Jahre alt. Seitens der Stadt gebe es eine große Bereitschaft „über denkbare Lösungsansätze zu verhandeln". Seine Wunschlösung wäre, dass Vernunft einkehre beim Eigentümer. Dieser könne zum Beispiel ein Krankenhaus in der Region beauftragen die Akten zu sichten und für die weiter aufzubewahrenden einen Raum zur Verfügung zu stellen, „damit man mal einen Strich unter die Sache bekommen könnte" (Bauernfeind/dpa, Nach Datenskandal durch YouTuber: Gericht befasst sich mit Akten in alter Klinik, www.heise.de 18.12.2022, Kurzlink: https://heise.de/-7398294).

Rheinland-Pfalz

Daten von Flüchtlingen und Volkszählungsverweigerern nach Cyberangriff im Darknet

Nach erfolglosen Lösegeldforderungen hat eine Ransomware-Gruppe gemäß der Mitteilung von Landrat Clemens Körner (CDU) vom Rhein-Pfalz-Kreis unter anderem Daten der Kreisverwaltung von Zensusverweigerern und ukrainischen Geflüchteten im Darknet veröffentlicht. Es wurden strafrechtliche Ermittlungen gegen die Cyberkriminellen, die sich Ransomware Vice Society nennen, eingeleitet, die ca. 600 Rechner des Landkreises gehackt haben sollen. Unter den gestohlenen Informationen befinden sich unter anderem Daten von 54 Zensusverweigerern sowie Namen, Anschriften und Geburtsdaten von ukrainischen Geflüchteten, die in dem Landkreis untergebracht wurden.

Die Kreisverwaltung arbeitet mit allen beteiligten Behörden und der Polizei zusammen, um Gegenmaßnahmen durchzuführen. Nachdem die Website der Kreisverwaltung am 11.11.2022 noch nicht wieder vollumfänglich erreichbar war, stellte diese eine Behelfsseite mit Informationen über den Vorfall zusammen und erklärte dort, dass die Verwaltung weder telefonisch noch per E-Mail erreichbar sei und Bürger ihre Anliegen der Kreisverwaltung in der Zwischenzeit über ein einfaches Webformular mitteilen könnten. Andere Kontaktmöglichkeiten seien die persönliche Vorsprache oder die Nutzung des Bürgertelefons mit der Rufnummer 115.

Der Landrat begründete die Verweigerung der Lösegeldzahlung damit, dass dies oft dazu führe, dass noch höhere Forderungen gestellt werden, weshalb Experten von einer Zahlung abraten. „Nach dem aktuellen Stand der Technik" erfülle man einen hohen Sicherheitsstandard. Eine 100-prozentige Sicherheit gäbe es nicht. Trotz großer Sicherheitsmaßnahmen sei es zu dem Cyberangriff gekommen, wie das Landeskriminalamt bestätigte. In einem offenen Brief hatte sich Körner umgehend an die Bevölkerung gewandt. Bei der Hackergruppe handele es sich „um eine hochprofessionelle und organisierte Gruppe, die aus Cyberangriffen ein regelrechtes Geschäftsmodell" gemacht habe (Koch/Eikenberg, Nach Cyberangriff auf Verwaltung: Daten ukrainischer Geflüchteter im Darknet, www.heise.de 11.11.2022, Kurzlink: https://heise.de/-7337774).

Datenschutznachrichten aus dem Ausland

Weltweit

Fast ½ Milliarde WhatsApp-Konten geleakt

Mitte November 2022 wurde von einem Nutzer eines Hacker-Forums gemäß Presseberichten eine Datenbank aus dem gleichen Jahr mit Telefonnummern von 487 Millionen WhatsApp-Nutzern zum Verkauf gestellt. Die Nummern stammen wohl aus 84 Ländern. Dem Leak zufolge sind darunter mehr als 6 Millionen Nummern aus Deutschland. Gemäß den Berichten konnten Nummern eingesehen und WhatsApp-Nutzern zugeordnet werden. Das Leak scheint also echte Daten zu beinhalten. Der Verkäufer versichert, dass alle Nummern zu aktiven Konten gehören. WhatsApp-Eigner Meta gab zunächst kein Statement zu dem Vorfall.

Unklar ist, woher die Datenbank stammt. Der Verkäufer gab nur an, dass er über „seine Strategie" an die Daten gekommen sei. Der Inhalt der Datenbank könnte Cybernews zufolge aus Scraping stammen, was die Nutzungs-

bedingungen von WhatsApp verbieten. Dabei extrahieren Kriminelle mit Scraping-Tools Daten von Websites oder -diensten. Mit 45 Millionen stammt der Großteil der Nummern aus Ägypten. Aber auch Italien (35 Millionen), die USA (32 Millionen) und Frankreich (20 Millionen) sind mit unzähligen Nummern in der Datenbank vertreten. Über den Preis der Datenbank wurde zunächst nichts bekannt. Auch ob sie bereits verkauft wurde, ist unklar. Die Telefonnummern könnten Angreifer etwa für Betrug und Phishing-Attacken missbrauchen (Schirrmacher, Angeblich 487 Millionen Telefonnummern über WhatsApp geleakt, www.heise.de 25.11.2022, Kurzlink: https://heise.de/-7352670).

EU

Ministerrat legt Position zu EUid fest

Die im EU-Ministerrat organisierten Regierungen der EU-Staaten haben ihren Kurs für eine europäische digitale Identität (EUid) festgelegt. Sie unterstützen die Initiative der EU-Kommission, dass allen Bürgern und Unternehmen künftig digitale Brieftaschen zur Verfügung stehen müssen. In diesen „E-Wallets" sollen die Nutzenden ihre nationale elektronische Identität (eID) speichern und mit Nachweisen anderer persönlicher Attribute wie Führerschein, Abschlusszeugnissen, Geburts- oder Heiratsurkunde und ärztlichen Rezepten verknüpfen können.

Die Kommission hatte ihren Verordnungsentwurf für eine europäische digitale Identität (EUid) im Sommer 2021 vorgelegt. Der Ministerrat, in dem je ein Minister jedes EU-Staates sitzt, hat zu dieser Skizze zur Reform der eIDAS-Verordnung seine Position mit Änderungswünschen fixiert (s.o. S. 37). Umstritten war im Vorfeld, dass die persönliche Wallet und eID mit einem lebenslangen eindeutigen Identifikator verbunden werden soll. Informationen aus zahlreichen Lebensbereichen könnten zusammengeführt werden und so die Bürger gläsern machen. Zwecks Abgleich von Datensätzen haben die Mitgliedstaaten „das Konzept der eindeutigen und dauerhaften Kennung" für die Online-Brieftaschen beibehalten. In der entsprechenden Definition stellen sie klar, dass dieses Personenkennzeichen „aus einer Kombination mehrerer nationaler und sektoraler Kennungen bestehen kann".

Der Rat hebt hervor, „dass der Abgleich von Datensätzen durch eine qualifizierte elektronische Bescheinigung von Attributen erleichtert werden kann". Zugleich schlägt er eine Klausel vor, wonach die Mitgliedstaaten den Schutz personenbezogener Daten gewährleisten und die Erstellung von Nutzerprofilen verhindern müssen. Wie dies gehen soll, bleibt offen. IT-Sicherheitsexperten und der Bundesdatenschutzbeauftragte Ulrich Kelber warnen, dass bei einer universellen Wallet mit einer „staatlich signierten Ausweiskopie" profilübergreifendes Tracking drohe. Bei den geplanten EUid müsse besonders darauf geachtet werden, dass diese „nicht mit einheitlichen Personenkennzeichen verknüpft" werden.

Der Rat erwartet, dass die sichere Speicherung kryptografischen Materials nur auf Basis einer Cybersicherheitszertifizierung zulässig wird. Prinzipiell soll ein „Secure Element" die IT-Sicherheit auf einem Mobilgerät gewährleisten. Auf dieses Element setzt auch die hiesige Smart-eID-Lösung für den Online-Ausweis auf dem Handy. Solche speziellen Chips sind bisher nur in den wenigsten Modellen verfügbar. Der Rat will daher auch zertifizierte andere Speicherlösungen wie Sicherheitstoken zulassen.

Der Ministerrat will die Absprache zwischen beteiligten Parteien modifizieren. In der Regel soll das Verfahren, mit dem eine Seite ihre Absicht mitteilt sich auf die Wallet zu verlassen, kosteneffizient und risikoadäquat sein. Für die Verarbeitung sensibler persönlicher Daten soll ein strengeres Registrierungs- oder Genehmigungsverfahren einzuhalten sein. Der Rat betont, dass Ausstellung, Verwendung zur Authentifizierung und Widerruf von E-Brieftaschen für natürliche Personen kostenlos sein sollen. Gebühren dürfen aber Dienstebetreibern verrechnet werden, wenn sie EUid-Wallets zur Authentifizierung heranziehen.

Das EU-Parlament muss seine Linie noch festzurren. Im Anschluss starten die Verhandlungen zwischen den Gesetzgebungsgremien über einen finalen Kompromiss. Ivan Bartos, tschechischer Vizepremierminister für Digitalisierung und Mitglied der Piratenpartei, zeigte sich im Namen der Ratspräsidentschaft überzeugt, dass die EUid unverzichtbar sei: „Wir stehen vor einem massiven Fortschritt in der Art und Weise, wie die Menschen ihre Identität und ihre Ausweise im täglichen Kontakt mit öffentlichen und privaten Einrichtungen verwenden und wie sie digitale Dienste nutzen. Dabei behalten sie stets die Kontrolle über ihre Daten."

Der ebenfalls zu den Piraten gehörende EU-Abgeordnete Patrick Breyer schlug dagegen Alarm: Die EUid dürfe „nicht zu einem digitalen Tagebuch auf Basis einer lebenslangen Identifikationsnummer werden, mit der unser digitales Leben erfasst und überwacht werden kann". Anonymität und Pseudonyme seien unverzichtbar. Auch die Bürgerrechtsorganisation Epicenter.works sprach von „beispiellosen Risiken für die Privatsphäre". Mit der eindeutigen Kennung sei jede Nutzertransaktion „für den Mitgliedstaat zentral beobachtbar, sodass eine panoptische Sicht auf alle Lebensbereiche entsteht". Die Diskussion liegt nun beim EU-Parlament (Krempl, EUid: EU-Rat stimmt für Online-Ausweis mit eindeutigem Personenkennzeichen, www.heise.de 06.12.2022, Kurzlink: https://heise.de/-7368464; siehe dazu auch den Offenen Brief auf S. 37).

EU

Regierungen blockieren parlamentarische Spionage-Aufklärung

Im Juli 2021 hatte ein Konsortium von Investigativ-Journalisten Berichte über den Missbrauch der Spionagesoftware Pegasus des israelischen Herstellers NSO durch Staaten in aller Welt veröffentlicht (DANA 3/2021, 187 f). Unter den Abgehörten befanden sich auch mehrere europäische Staatschefs. Um die Vorwürfe zu klären, hat das EU-Parlament im März 2022 einen Untersuchungsausschuss eingerichtet; am 08.11.2022 stellte die Berichterstatterin des Ausschusses, Sophie in't Veld, die bisherigen Erkenntnisse vor. Demzufolge nutzen so gut wie alle EU-Mitgliedstaaten Spionagesoft-

ware. Allein der Hersteller NSO gab an 14 Kunden in der EU zu haben, zweien von ihnen sei gekündigt worden.

Sophie in't Veld nennt den Spionage-Skandal ein europäisches „Watergate". Watergate war der bislang größte US-amerikanische Abhörskandal, bei dem die regierenden Republikaner Anfang der 70er-Jahre unter Richard Nixon das Büro der Demokratischen Partei mit Wanzen abhörten. Seitdem ist die Abhörtechnik um einiges raffinierter geworden. Programme machen Handys zu Wanzen.

Bei der parlamentarischen Untersuchung geht es um die weitgehend unkontrollierte Nutzung von digitaler Spionagesoftware durch Staaten in Europa. Dabei stehen fünf Länder im Fokus des Berichts. In Zypern haben sich demnach viele Firmen angesiedelt, die Spyware herstellen, weil es dort vergleichsweise laxe Regeln gibt. In Spanien (DANA 3/2022, 190 f.), Griechenland, Polen (DANA 1/2022, 47) und Ungarn wurde Spyware in großem Stil eingesetzt. In Spanien richtete sich die Überwachung vorwiegend gegen Politiker in Katalonien, die sich für eine Unabhängigkeit von Spanien einsetzten, in Ungarn und Polen fand sich Spionagesoftware auf Telefonen von Oppositionellen oder Journalisten, was ein eklatanter Verstoß gegen europäische Werte und individuelle Rechte der Betroffenen ist.

Rechtlich unterliegt die Nutzung von Überwachungssoftware durch Ermittlungsbehörden strengen Regeln. Doch in einigen Mitgliedstaaten werden diese dem vorläufigen Bericht zufolge bewusst vage formuliert oder gezielt ausgehöhlt. Der jüngste Abhörskandal plagt Griechenland (DANA 4/2022, 269 f.). Dort veröffentlichten Medien eine Liste mit 33 Opfern, die mit der Spyware Predator des Herstellers Intellexa ausgespäht wurden, darunter hauptsächlich Politiker und Journalisten. Auch die EU-Kommission selbst wurde dem Bericht zufolge Opfer von Abhör-Attacken.

Dennoch musste sich der PEGA-Ausschuss bei seiner Arbeit weitgehend auf öffentliche Quellen stützen. Grund dafür seien zum einen mangelnde Befugnisse von Untersuchungsausschüssen des EU-Parlaments. Der Ausschuss kann niemanden vorladen. Falschaussagen sind nicht strafbar. Der andere Grund ist in't Veld zufolge die unzureichende Kooperationsbereitschaft der EU-Länder, die auf Fragen des Ausschusses meist mit Verweis auf die nationale Sicherheit nicht antworten wollten. Im Juli 2022 hatte der Ausschuss den Mitgliedstaaten einen Fragenkatalog zur Nutzung von Spyware geschickt. Die äußerst ausweichende Antwort durch den Europäischen Rat kam erst am Abend vor der Veröffentlichung des vorläufigen Berichts.

Auch die Kommission leistete in't Veld zufolge keinen signifikanten Beitrag zur Aufklärung, obwohl rund 60 Mitarbeiter der Kommission mit Spähsoftware attackiert worden sein sollen, darunter auch der belgische Kommissar für Justiz, Didier Reynders. Genauere Informationen verweigere die Kommission mit Verweis auf ihre eigene Sicherheit. Angreifer könnten zu viel über die Abwehrfähigkeiten der Kommission erfahren.

Diese Abwehrfähigkeiten stellt in't Veld, die für die niederländische Partei D66 im EU-Parlament sitzt, infrage. Die EU sei schnell dabei sich zu verteidigen, wenn die Bedrohung von außen komme, seien es Fake News oder drohende Hassrede auf Twitter. Doch habe die Europäische Union ein Problem, wenn es darum gehe Bedrohungen von innen abzuwehren: „Wenn die Bedrohung nicht von irgendwem da draußen kommt, sondern von Regierungen der Nationalstaaten, ist die Kommission auf einmal der Ansicht, dass die Verteidigung der europäischen Werte keine europäische Angelegenheit ist, sondern Aufgabe der Nationalstaaten." Die Nutzung von Spyware in der EU sei alles andere als eine nationale Frage, erst recht, wenn Opfer in der Kommission und im Parlament säßen und Täter im Europäischen Rat. In't Veld erklärte, sie hoffe, dass die Erkenntnisse aus dem vorläufigen Bericht einige Staaten ermutigen sich doch noch an der Aufklärung zu beteiligen. Der Abschlussbericht des Ausschusses wird im März 2023 erwartet (zum Einsatz in Deutschland DANA 4/2021, 239 ff; Israel DANA 2/2022, 118 f. u. 1/2022, 49 ff.; USA DANA 1/2022, 53 f.; Muth, Spionieren unter Nachbarn, SZ 09.11.2022, 7).

EU/Irland

EDSA zwingt irische DPC zu Sanktionierung von Meta

Meta Platforms darf gemäß dem Beschluss des Europäischen Datenschutzausschusses (EDSA) vom 05.12.2022 keine Personendaten für Werbezwecke ohne explizite Einwilligung der Betroffenen nutzen. Die im EDSA vertretenen Aufsichtsbehörden überstimmten damit die irische Datenschutzbehörde, die Data Protection Commission (DPC), und verpflichteten diese eine Strafe zu verhängen. Im Januar 2023 verhängte die DPC, die das Verfahren vier Jahre hinausgezögert hatte, daraufhin ein Bußgeld in Höhe von 390 Mio. Euro, was nach Ansicht des Beschwerdeführers viel zu wenig ist.

• Werbeauswertung ist illegal

In der Entscheidung geht es um Datenschutzbestimmungen, die Meta Platforms bei Facebook, Instagram und WhatsApp anwendet. Für die Auswertung des Nutzerverhaltens auf fremden Webseiten und Apps bietet Meta eine Opt-Out-Option an. Für die Auswertung der auf Facebook und Instagram selbst anfallenden Daten haben User bislang jedoch keine Wahl. Seit 2018 gilt die Datenschutz-Grundverordnung (DSGVO). Diese legt fest, unter welchen Bedingungen personenbezogene Daten genutzt werden dürfen. In einigen Fällen geht das ohne explizite Zustimmung, insbesondere dann, wenn Daten ausgewertet werden müssen, um die Leistung erbringen zu können: Wer sich z.B. etwas liefern lässt, muss akzeptieren, dass der Bote die Lieferadresse erfährt. Facebook (heute Meta Platforms) versuchte diese Bestimmung auszunutzen: Am 25.05.2018, dem Zeitpunkt des Inkrafttretens der DSGVO, erklärte der Datenkonzern in seinen Nutzungsbedingungen die Berieselung mit persönlich zugeschnittener Werbung zum Teil des Dienstes, so z.B. in der aktuellen Fassung für deutsche Facebook-User:

„Wir helfen dir, Inhalte, Produkte und Dienste zu entdecken, die dich möglicherweise interessieren: Wir zeigen

dir personalisierte Werbeanzeigen, Angebote und sonstige gesponserte oder kommerzielle Inhalte, um dir dabei zu helfen, Inhalte, Produkte und Dienste zu entdecken."

Die von Max Schrems gegründete europäische Datenschutzorganisation noyb legte noch im Mai 2018 Beschwerde bei der irischen Datenschutzbehörde, der DPC, ein. Meta Platforms unterhält seinen Europasitz in Irland, weshalb die DPC zuständig ist. Eine weitere Beschwerde kam von einem belgischen Staatsbürger. Fortan argumentierte Meta, die Auswertung personenbezogener Daten sei nicht bloß zulässig, nein, es schulde diesen „Dienst" seinen Nutzern, was die DPC unterstützte. Laut Meta gab es während des laufenden Verfahrens zehn vertrauliche Treffen mit der Behörde, an denen der Beschwerdeführer nicht teilnehmen durfte, was noyb kritisiert: „Aufgrund der mitunter grotesken Verfahrensführung durch die DPC dauerte der Fall mehr als 4,5 Jahre und führte zu Hunderten von Seiten an Berichten und Stellungnahmen, obwohl es sich um eine recht einfache Rechtsfrage handelte."

• DPC Irland deckt Facebook/Meta

2021 machte noyb öffentlich, dass die DPC sogar versucht hat die Leitlinien des Europäischen Datenschutzausschusses (EDSA) für die Auslegung der DSGVO im Sinne Metas zu beeinflussen. Im EDSA kommen der Europäische Datenschutzbeauftragte und die Datenschutzbehörden des EWR (Europäischer Wirtschaftsraum) zusammen; Stimmrecht haben nur EU-Mitglieder. Am 05.12.2022 tagte der EDSA zum 72. Mal. Einziger Tagesordnungspunkt war die Sicherstellung der einheitlichen Anwendung europäischen Datenschutzrechts bei in Irland gegen Meta anhängigen Verfahren, nämlich je einem zu Facebook, Instagram und WhatsApp. Der EDSA lehnte den Bescheidentwurf der irischen Kollegen ab, mit dem Facebooks Einwilligungstrick abgenickt werden sollte. Stattdessen ordnet der EDSA die irische DPC an Metas Regeln für rechtswidrig zu befinden und innerhalb eines Monats eine Strafe zu verhängen. Gegen den Bescheid dürfte Meta dann vor Gericht ziehen, was die Sache weitere Jahre hinauszögern dürfte.

Die Freude bei Schrems über die EDSA-Entscheidung war eher verhalten: „In diesem Fall geht es um eine einfache Rechtsfrage, die aber endlos verzögert wurde. Trotz des langwierigen Verfahrens freuen wir uns über die Entscheidung des Europäischen Datenschutzausschusses." Allerdings könnten die Gerichtsverfahren noch geraume Zeit dauern. Schrems ärgert zudem, dass der Erlös aus der Strafe an Irland fließt – jenen Staat, der das Verfahren lange verzögert und sich an die Seite Metas gestellt hat. Unterliegt Meta auch vor Gericht, droht eine saftige Milliardenstrafe, da der Trick mit den Nutzungsbedingungen als vorsätzliche Verletzung der DSGVO ausgelegt werden könnte. Gemäß Presseberichten hat Metas Irlandtochter ihre Rücklagen für Datenschutzstrafen bereits 2021 von zwei auf drei Milliarden Euro aufgestockt.

Für Werbeplattformen, die sich an die DSGVO-Auslegung des EDSA halten, wäre eine Verurteilung Metas eine gute Nachricht. Die Gelddruckmaschine Metas müsste einen Gang zurückschalten. Legal bleibt Werbung kontextbasiert auszuspielen. So darf Meta neben einem Video eines Squash-Ballwechsels Werbung für Squashschläger zeigen. Das zielt zwar auch auf die vermeintlichen Interessen der Zuschauer ab, aber ohne deren Verhalten abseits der aktuellen Ansicht oder sonstige personenbezogene Daten heranzuziehen. Meta kündigte an gegen das Bußgeld Einspruch einzulegen.

• noyb: Bußgeld ist viel zu niedrig

Nachdem der EDSA seine Entscheidungen in den beiden Fällen veröffentlicht hatte kritisierte Schrems und sein Verein noyb die Bußgeldhöhe. Meta komme mit der Strafe von insgesamt 390 Millionen Euro, die die irische Datenschutzbehörde jüngst gegen den US-Konzern verhängt hat, viel zu billig davon. Die DPC hätte Meta mit der möglichen Höchststrafe von 4,36 Milliarden Euro belegen müssen, so noyb: „Die DPC ignorierte die von Meta erzielten, rechtswidrigen Einnahmen." Die Behörde habe sich nicht veranlasst gesehen auch nur eine Schätzung vorzunehmen. Schrems: „Jeder weiß von Metas enormen Einnahmen durch Werbung." Die irische Behörde habe nicht einmal von ihren gesetzlichen Befugnissen Gebrauch gemacht den Plattformbetreiber um diese Informationen zu bitten. noyb habe die einschlägigen Daten recherchiert und „in einer Stunde berechnen" können, „dass die Geldstrafe um 3,97 Milliarden Euro höher sein müsste".

Nach eigenen Angaben hat das börsennotierte Meta zwischen dem dritten Quartal 2018 und dem dritten Quartal 2022 84,7 Milliarden Euro mit Werbung auf dem europäischen Kontinent eingenommen. Heruntergerechnet auf EU-Nutzer ergibt dies rund 72,5 Milliarden Euro. Selbst wenn es sich dabei nicht nur um Umsätze aus personalisierter Werbung handle, geht noyb davon aus, dass diese um ein Vielfaches höher lagen als die nicht verhängte Höchststrafe.

Der EDSA hatte die irische Aufsicht angewiesen, dass die Sanktion „den entstandenen Vorteil aus der rechtswidrigen Verarbeitung" widerspiegeln müsse und hatte gefordert „eine Geldstrafe zu verhängen, die diesen Betrag übersteigt".

Dieser Auflage widersetzte sich, so Schrems, die DPC. Die Behörde habe Meta so „gut 4 Milliarden Euro geschenkt". Laut der DSGVO müssen Sanktionen generell „wirksam, verhältnismäßig und abschreckend" sein und den „finanziellen Nutzen aus dem Verstoß" berücksichtigen. Der Ermessensraum endet bei einem Konzern bei 4 Prozent des weltweiten Umsatzes des vergangenen Jahres. Im Fall von Meta würde dies einer Höchststrafe von 4,36 Milliarden Euro entsprechen, die laut Schrems angesichts der Werbeumsätze des Unternehmens auch in jedem Fall fällig gewesen wäre.

Die DPC hatte in ihren Entscheidungsentwürfen zunächst eine Geldbuße von maximal 36 Millionen Euro für Facebook und 23 Millionen Euro für Instagram vorgesehen. Erst nach der Intervention des EDSA setzte sie diese auf 210 und 180 Millionen Euro hoch. Die Bürgerrechtler von noyb drängen den EDSA seine bereits erteilten Vorgaben vollständig durchzusetzen. Sonst hätte es sich für Meta „absolut gelohnt gegen die DSGVO zu verstoßen".

• Nicht das Ende vom Lied

Weitere gerichtliche Auseinandersetzungen zeichnen sich in dem Streit ab.

So wies der EDSA die DPC bereits an eine neue Untersuchung durchzuführen, die sich auf alle Datenverarbeitungsvorgänge von Facebook und Instagram erstreckt. Sie soll besondere Kategorien personenbezogener Daten einschließen, die im Zusammenhang mit diesen Vorgängen verarbeitet werden können oder nicht.

Die DPC will dem nicht nachkommen und kündigte an eine Nichtigkeitsklage beim Europäischen Gerichtshof einzureichen, um die Aufhebung der Direktive des EDSA zu erreichen. Dieser habe „keine allgemeine Aufsichtsfunktion". Dem Ausschuss stehe es nicht zu „eine Behörde anzuweisen, unbefristete und spekulative Untersuchungen durchzuführen". Alles andere wäre nicht mit den in der DSGVO festgelegten Kooperations- und Kohärenzregelungen vereinbar (Sokolov, EU lehnt Facebook-Trick ab: Werbung ist keine Leistung, DSGVO-Strafe folgt, www.heise.de 06.12.2022, Kurzlink: https://heise.de/-7368428; Strafe gegen Meta-Konzern, SZ 05./06.01.2023; Krempl, Beschwerdeführer: Irische DSGVO-Strafe für Meta müsste 4 Milliarden höher sein, www.heise.de 18.01.2023, Kurzlink: https://heise.de/-7463309).

EU/Irland

265-Millionen-Strafe gegen Meta wegen Facebook-Datenabfluss

Die irische Datenschutzbehörde Data Protection Commission (DPC) teilte am 28.11.2022 mit, dass sie gegen die irische Niederlassung der Facebook-Mutter Meta eine Strafe in Höhe von 265 Millionen Euro verhängt hat, weil Facebook 2018 nicht ausreichend verhindert hat, dass insgesamt etwa 533 Millionen Datensätze mit persönlichen Informationen von Facebook-Nutzenden abgegriffen und veröffentlicht worden sind. Meta muss danach eine Reihe von Abhilfemaßnahmen treffen, um die Datenverarbeitung in Einklang mit den Bestimmungen der Datenschutz-Grundverordnung (DSGVO) zu bringen. Die DPC hatte im April 2021 eine Untersuchung gegen Meta eingeleitet, nachdem im gleichen Monat erneut Telefonnummern, E-Mail-Adressen und weitere Daten von Facebook-Nutzenden im Internet veröffentlicht worden waren. 2018 bestätigte Facebook, dass Nutzerdaten des Online-Netzwerks über Facebooks Entwickler-API durch automatische Abrufe systematisch eingesammelt werden konnten. 2019 waren 419 Millionen solcher Datensätze im Internet aufgetaucht.

Facebook hatte behauptet, dass die im April 2021 aufgetauchten Daten vor Mai 2018 abgegriffen worden seien, bevor das Unternehmen den Zugriff technisch eingeschränkt hatte. Den Untersuchungen der Datenschützer zufolge stammte jedoch ein Großteil der Daten aus dem Jahr 2019. Entsprechend sieht die DPC einen Verstoß gegen Artikel 25 Abs. 1 u. 2 DSGVO. Meta habe es unterlassen geeignete technische und organisatorische Maßnahmen zu treffen, um die Einhaltung der DSGVO-Verpflichtung zum Datenschutz durch Design und Standard einzuhalten.

Nach Angaben der DPC ist das „umfassende Untersuchungsverfahren" in Kooperation mit sämtlichen Datenschutzbehörden der EU erfolgt. Sie hätten der Entscheidung der DPC am 25.11.2022 zugestimmt. In der Entscheidung sei neben der Strafe ein Verweis und eine Anordnung ausgesprochen worden. Meta müsse nun innerhalb eines festgelegten Zeitrahmens Abhilfemaßnahmen schaffen. Seit September 2021 hat die DPC mehrere Strafen wegen potenzieller Datenschutzverstößen gegen die irische Meta-Niederlassung verhängt, die sich inzwischen auf insgesamt etwa 910 Millionen Euro belaufen. Darunter fallen Strafen gegen WhatsApp und Instagram. Gegen diese hat Meta Rechtsmittel eingelegt, Urteile stehen noch aus (Bünte, Facebook-Scraping: Irische Datenschützer verhängen Millionenstrafe gegen Meta, www.heise.de 28.11.2022, Kurzlink: https://heise.de/-7358898).

EU/Irland

DPC: Mini-Bußgeldbescheid für WhatsApp

Die irische Datenschutzbehörde, die Data Protection Commission (DPC), hat nach Facebook und Instagram auch WhatsApp wegen dessen Praxis der „Zwangseinwilligung" in eine breit gefasste Verarbeitung personenbezogener Informationen von Nutzern mit einem Bußgeld in Höhe von 5,5 Millionen Euro bestraft. Der Messaging-Anbieter, der wie die anderen beiden Plattformbetreiber zum US-Konzern Meta gehört, kommt dabei glimpflich davon: Facebook soll 210 und Instagram soll 180 Millionen Euro zahlen, was Kritiker bereits als viel zu niedrig ansehen (s.o.).

Alle drei Fälle brachte der österreichische Datenschutzaktivist Max Schrems mit seiner Organisation noyb in die Gänge. Diese reichte die Beschwerden gegen die den Nutzern abgeforderte „Zwangseinwilligung" im Mai 2018 direkt nach Wirksamwerden der Datenschutz-Grundverordnung (DSGVO) ein. Im Fall von WhatsApp agierte noyb dabei im Namen eines deutschen Users. Der Kernvorwurf lautete jeweils, die Dienste hätten datenhungrige Services wie gezielte Werbung als Leistung für die Nutzer ausgegeben und die Zustimmung zum Online-Tracking einfach in die Allgemeinen Geschäftsbedingungen eingebaut.

Mit ihrer neuen Entscheidung bestätigt die DPC, dass Meta WhatsApp-Nutzende nicht zwingen darf die Verwendung ihrer Daten für „Serviceverbesserungen" und „Sicherheitsfunktionen" mit abzunicken. Den wesentlichen Punkt der Verarbeitung der persönlichen Informationen für „verhaltensbezogene Werbung, für Marketingzwecke sowie für die Bereitstellung von Statistiken an Dritte und den Austausch von Daten mit verbundenen Unternehmen" behandelte die Behörde gar nicht. Der Europäische Datenschutzausschuss (EDSA) als übergeordnetes Gremium hatte die DPC aber aufgefordert auch diese Fragen mit zu untersuchen.

WhatsApp bietet selbst zwar keine personalisierte Werbung an. noyb geht aber davon aus, dass der Anbieter Metadaten an Facebook und Instagram weitergibt, die wiederum dort für gezielte Reklame verwendet werden. Diese Verbindungs- und Standortdaten gäben viele Informationen über das Kommunikationsverhalten der Nutzer und ihr soziales Gefüge preis, etwa wer mit wem wann kommuniziert, wer

die App wann, wie lange und wie oft nutzt. Im Gegensatz zu den ausgetauschten Inhalten sind die Metadaten unverschlüsselt. Schrems zeigte sich erstaunt, wie die DPC nach einem 4,5-jährigen Verfahren und den damit verknüpften Kosten „den Kern des Falles einfach ignoriert". Auch die verbindliche Entscheidung des EDSA habe die Aufsichtsinstanz offensichtlich nicht beachtet. Man könnte glauben, dass die DPC endgültig alle Verbindungen zu den anderen EU-Behörden und zu den Anforderungen des EU- und des irischen Rechts kappe und außerdem den Partnern „endgültig den Stinkefinger" entgegenstrecke. Die vom EDSA in Auftrag gegebenen weitergehenden Untersuchungen lehnt die irische Behörde – genauso wie bei Facebook und Instagram – ab. Soweit das Gremium seine Befugnisse überschreiten könnte, hält sie es für angemessen „eine Nichtigkeitsklage vor dem Europäischen Gerichtshof zu erheben".

WhatsApp kündigte an die Entscheidung der DPC anzufechten: „Wir sind der festen Überzeugung, dass die Art und Weise, wie der Dienst funktioniert, sowohl technisch als auch rechtlich konform ist." Der EDSA überstimmte in der Auseinandersetzung den Beschlussentwurf der irischen Aufsicht zum sechsten Mal in Folge und drängte auf Verschärfungen. Die DPC gilt seit Langem als „Flaschenhals" bei der DSGVO-Umsetzung in der ganzen EU (Krempl, „Stinkefinger": WhatsApp kommt bei Einwilligungstrick mit kleiner Strafe davon, www.heise.de 19.01.2023, Kurzlink: https://heise.de/-7464806).

EU/USA

Transatlantischer Datenschutz-Rahmen vorgelegt

Die EU-Kommission hat am 13.12.2022 nach fast eineinhalb Jahren Verhandlungen mit der US-Regierung ihren Vorschlag für einen neuen Angemessenheitsbeschluss veröffentlicht. Auf insgesamt 134 Seiten wird dem um die US-Präsidialverfügungen vom Oktober 2022 erweiterten US-Datenschutzrecht ein angemessener Schutz personenbezogener Daten nach Artikel 45 DSGVO attestiert, wenn Unternehmen sich dem sogenannten transatlantischen „EU-US-Data Privacy Framework" (TDPF) unterwerfen. Wenn der Angemessenheitsbeschluss in den kommenden Monaten finalisiert wird, können Unternehmen und andere Organisationen sich den Bestimmungen unterwerfen und über das sogenannte TDPF personenbezogene Daten aus der EU in den USA verarbeiten.

Die EU-Kommission begründet ihren Entwurf eines Angemessenheitsbeschlusses umfangreich: Der Europäische Gerichtshof habe klargestellt, dass es für einen solchen kein identisches Schutzniveau benötige. Das allerdings war nie umstritten, sondern vielmehr, ob in den USA dem Anspruch eines funktional äquivalenten Datenschutzes zum EU-Niveau ausreichend nachgekommen wird. Zweimal stellten die Richter des Europäischen Gerichtshofes (EuGH) in Luxemburg fest, dass dies auch mit zusätzlichen Zusicherungen nicht der Fall war. EU-Justizkommissar Reynders, der die Verhandlungen mit der US-Regierung leitete, hofft, dass es dieses Mal klappt.

US-Präsident Joe Biden hatte in seiner Executive Order 14086 unter anderem Maßnahmen angeordnet, mit denen die US-Nachrichtendienste zu Änderungen bei der Signalaufklärung verpflichtet werden. So sollen die US-Dienste künftig bei ihren Datensammlungen darauf achten, dass diese „notwendig und verhältnismäßig" sind, und bei ihren Datensammlungen besser kontrolliert werden. Zudem soll auch ein Zwei-Kammer-Rechtsweg für Nicht-EU-Bürger offenstehen, mit dem Einwände geltend gemacht werden können.

Wie bei den beiden vorangegangenen Versuchen den USA ein angemessenes Datenschutzniveau zu bescheinigen, ist auch diesmal kein Automatismus vorgesehen. US-Unternehmen, die unter das EU-US-Data Privacy Framework schlüpfen wollen, müssen sich bei der Handelsaufsicht, der Federal Trade Commission (FTC), registrieren lassen und die damit verbundenen Verpflichtungen akzeptieren. Die FTC ist als Aufsichtsbehörde rechtlich in der Lage Verstöße gegen Selbstverpflichtungen hart zu ahnden.

Zur Angemessenheitsentscheidung der EU-Kommission müssen im nächsten Schritt Stellungnahmen der Mitgliedstaaten und der europäischen Datenschutzaufsichtsbehörden erfolgen. Letztere haben allerdings kein Einspruchsrecht. Auch das Europaparlament hat Mitberatungsrechte. Allerdings kann es den Entwurf formal nicht verhandeln, sondern nur über ein Einspruchsverfahren komplett verhindern, was als unwahrscheinlich gilt. Die EU-Kommission will das Verfahren in wenigen Monaten abschließen.

Aus Sicht der Internetwirtschaft ist der Entwurf der Kommission ein guter Schritt, Oliver Süme, Vorstand des Verbands Eco: „Insbesondere für viele kleine und mittelständische Unternehmen in Europa ist ein rechtssicherer Datenaustausch auf internationaler Ebene die Basis für ihre datengetriebenen Geschäftsmodelle." Er hoffe auf eine zeitnahe Verabschiedung des Angemessenheitsbeschlusses. Der österreichische Datenschutzaktivist Max Schrems, der schon die Vorgängervereinbarungen Safe Harbor und Privacy Shield vor dem EuGH zu Fall brachte, wird den vorgeschlagenen Angemessenheitsbeschluss prüfen: „Da sich der Entscheidungsentwurf auf die bereits bekannte Executive Order stützt, glaube ich kaum, dass diese einer Anfechtung vor dem Gerichtshof standhalten wird." Ob Schrems damit Recht behält, werden absehbar die Luxemburger Richter prüfen müssen. EU-Justizkommissar Didier Reynders zeigte sich verhalten optimistisch, dass der dritte Anlauf diesmal dort Bestand haben könnte. Dem Entwurf sind wieder zahlreiche Schreiben von US-Stellen beigefügt, etwa die Ausführungen des Department of Commerce, der Chefin der US-Handelsaufsicht FTC Lina Khan, des US-Justizministeriums und der Behörde des Direktors der Nachrichtendienste (ODNI). In den Schreiben wird erläutert, welche Zusicherungen die US-Seite gegeben hat und wie diese gemeint sind (vgl. Weichert, DANA 4/2022, 246 ff.; Steiner, „Privacy Shield"-Nachfolger: Vorschlag der EU-Kommission zur US-Datenspeicherung, www.heise.de 14.12.2022, Kurzlink: https://heise.de/-7393763; Muth, Daten wieder in die USA, SZ 14.12.2022, 15).

Frankreich

CNIL verhängt gegen Microsoft 60-Mio.-Euro-Bußgeld wegen Cookie-Einstellungen

Die französische Datenschutzbehörde CNIL (Commission Nationale de l'Informatique et des Libertés) hat am 19.12.2022 Microsoft ein Bußgeld in Höhe von 60 Millionen Euro auferlegt, weil es beim Suchen mit Bing keine einfache Option zum Ablehnen von Cookies gab. Sie begründet die Höhe des Bußgelds mit dem Umfang der erfolgten Datenverarbeitung und der Anzahl der betroffenen Personen. Eingepreist hat die Aufsichtsinstanz auch Gewinne, die der US-Konzern mit europäischem Hauptsitz in Irland aus Werbeeinnahmen erzielt habe. Berücksichtigt hat die CNIL dabei nach eigenen Angaben nur Einkünfte, die indirekt auf Daten beruhen, die Microsoft mithilfe von Cookies gesammelt hat.

Die Datenschützer hatten Kontrollen auf bing.com im September 2020 und Mai 2021 durchgeführt und stellten fest, dass bei Nutzern Cookies ohne Zustimmung auf den Endgeräten landeten, obwohl sie unter anderem Werbezwecken dienten. Es habe keine Schaltfläche gegeben, mit der Besucher das Setzen der Browserdateien „ebenso einfach ablehnen, wie akzeptieren" hätten können. Um über den Banner alle Cookies zurückzuweisen, waren zwei Klicks erforderlich; um sie entgegenzunehmen nur einer. Dieser verkomplizierte Ablehnungsmechanismus verleitete User den Prüfern zufolge dazu aus Bequemlichkeit die Zustimmungsschaltfläche im ersten Fenster zu bevorzugen.

Zusätzlich zu der Geldstrafe erließ die CNIL auch eine Anordnung, wonach das Unternehmen auf bing.com innerhalb von drei Monaten die Zustimmung von Personen einholen muss, die die Suchmaschine aus Frankreich ansteuern, bevor es auf ihrem Endgerät Cookies zu Werbezwecken ablegt und Tracker einsetzt. Bei einer verspäteten Umsetzung dieser Auflage droht Microsoft ein Zwangsgeld in Höhe von 60.000 Euro pro Tag. Die Behörde verweist darauf, dass die Bedingungen für das Einholen der Zustimmung der Nutzer lange rechtswidrig gewesen seien. Erst am 29.03.2022 habe der Konzern eine Schaltfläche „Alles ablehnen" eingeführt.

Die Sanktion verhängte die CNIL nicht auf Basis der Datenschutz-Grundverordnung (DSGVO), sondern auf Artikel 82 des nationalen Gesetzes über Informatik und Freiheiten, mit dem der französische Gesetzgeber die E-Privacy-Richtlinie der EU von 2002 umgesetzt hatte. Die französischen Kontrolleure mussten den Fall so nicht an die irische Datenschutzbehörde DPC weiterleiten, die nach der DSGVO federführend für Microsoft zuständig ist. Die CNIL verhängte zuvor aus vergleichbaren Gründen eine Strafe in Höhe von 100 Millionen Euro gegen Google, die der Conseil d'Etat im Januar 2022 abschließend bestätigte. Auch Facebook musste in Frankreich schon 60 Millionen wegen Opt-in-Problemen zahlen (Krempl, Cookie-Einwilligung: Microsoft muss 60 Millionen Euro in Frankreich zahlen, www.heise.de 22.12.2022, Kurzlink: https://heise.de/-7441411).

EU/USA

Microsoft passt DS-Regeln an

Mit Datum vom 01.01.2023 hat Microsoft eine überarbeitete Version seines Auftragsverarbeitungsvertrags mit einem „Microsoft Products and Services Data Protection Addendum" (DPA) veröffentlicht, mit dem der US-Konzern das Versprechen einer bereits Mitte 2021 angekündigten „EU-Datengrenze" offiziell umsetzt. Ziel ist es Transfers persönlicher Informationen von Kunden aus der EU in die USA möglichst zu vermeiden, nachdem der Europäische Gerichtshof (EuGH) den Privacy Shield gekippt hatte.

Im DPA heißt es: „Bei Online-Diensten mit EU-Datengrenze speichert und verarbeitet Microsoft die Kundendaten innerhalb der Europäischen Union, wie in den Produktbedingungen festgelegt." Wie weit diese Formulierung trägt, ist offen. Der US-Kongress hatte 2018 einen „Cloud Act" verabschiedet, der regelt, wie die Kooperation zwischen US-Strafverfolgungsbehörden und ausländischen Partnern und damit der Zugriff auf Daten ablaufen soll, die sich auf Servern außerhalb des eigenen Territoriums befinden. Für die Details sind bilaterale Abkommen vorgesehen.

Die EU-Gesetzgebungsgremien einigten sich im Juni 2022 prinzipiell auf eine gemeinsame Linie zur geplanten E-Evidence-Verordnung mit einschlägigen Rahmenbedingungen inklusive einiger Schutzklauseln, die auch für US-Anfragen gelten sollen. Der EuGH stellte bislang mehrfach fest, dass US-Gesetze wie der Foreign Intelligence Surveillance Act (FISA) oder der Cloud Act eine Massenüberwachung durch Sicherheitsbehörden ermöglichen und der Datenschutzstandard in den USA daher nicht dem in der EU entspricht.

In einem Anhang zu dem Nachtrag sichert Microsoft ferner explizit zu „die Rechenschaftspflichten des Kunden" nach der Datenschutz-Grundverordnung (DSGVO) zu unterstützen und die dafür nötige Produktdokumentation zur Verfügung zu stellen. Dies gelte für die gesamte Laufzeit des Abonnements des Kunden oder des entsprechenden Dienstleistungsauftrags. Nutzende sollten so leichter nachweisen können, dass sie etwa das Office-Paket Microsoft 365 datenschutzkonform einsetzen, erläutert der Rechtsanwalt Stefan Hessel von der Kanzlei Reuschlaw in einem Beitrag auf Microsofts Social-Media-Netzwerk LinkedIn. Dies ist höchst umstritten: Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK) unterstrich im November 2022, dass Einrichtungen wie Ämter, Schulen und Unternehmen die Suite für Büroanwendungen mit Cloud-Anschluss ohne Weiteres „nicht rechtskonform einsetzen" könnten. Sie müssten auf jeden Fall zusätzliche Schutzvorkehrungen treffen.

Microsoft und industrienahe Juristen wiesen die Bewertung der DSK brüsk zurück. Für manche dieser Beobachter drängte sich sogar die Frage auf, „ob die DSK rechtsstaatliche Grundsätze einhält". Eine behördliche Stellungnahme, in der Microsoft 365 letztlich als rechtswidrig bewertet werde, kommt einer Produktwarnung mit massiven Folgen

für Unternehmen gleich. Die Kritiker meinten, die Aufsichtsbehörden hätten „wichtige Meilensteine in puncto Drittstaatentransfer“ wie den angekündigten neuen EU-US-Rahmen oder die EU-Datengrenze abwarten sollen.

Aus Kreisen der Datenschutzbeauftragten ist dagegen zu hören, dass beide Seiten 14 mehrstündige Videokonferenzen mit Microsoft zuzüglich Vor- und Nachbereitung durchgeführt haben und die bisherigen Zusicherungen bis ins Detail untersucht worden sind. Microsoft habe sich dabei beharrlich geweigert alle Verarbeitungen zu beschreiben. Dies lege nahe, dass viele davon ohne Rechtsgrundlage erfolgten.

Für personenbezogene Daten, die Microsoft als Anbieter von Telekommunikationsdiensten verarbeitet und die so nicht unter die DSGVO fallen, stellt das Unternehmen zudem mit dem taufrischen DPA klar, dass es einschlägige gesetzliche Schutzvorgaben wie hierzulande das Fernmeldegeheimnis zu beachten gedenke: „Microsoft wird alle telekommunikationsspezifischen Gesetze und Vorschriften einhalten, die für die Bereitstellung der Produkte und Dienste gelten.“ Dies umfasse auch eine Benachrichtigung über Sicherheitsverletzungen und Datenpannen. Der Konzern hebt ferner hervor, dass auch die technischen und organisatorischen Schutzmaßnahmen aus den Standardvertragsklauseln (SVK) zwischen Microsofts europäischem Hauptsitz Irland und den Niederlassungen in den USA zum Einsatz kämen. Die Datenschutzergänzung gilt zudem nicht mehr nur für Kunden mit Volumenlizenzverträgen, sondern für alle mit einem bestehenden Produkt- und Dienstleistungsvertrag. Die neuen SVK der EU hatte das Unternehmen bereits bei der vorausgegangenen DPA-Änderung im September 2022 übernommen. Hessel rät Verantwortlichen sich unabhängig davon, ob der Nachtrag die Aufsichtsbehörden überzeuge, „um einen Abschluss des neuen DPA“ zu bemühen und die Klauseln in ihrer Datenschutzdokumentation zu berücksichtigen (Krempl, Datenschutzergänzung: Microsoft setzt „EU-Datengrenze“ um, www.heise.de 03.01.2023, Updated 04.01.2023, Kurzlink: https://heise.de/-7447136).

Italien

DSGVO-Bußgeld gegen Clubhouse-Betreiber

Die italienische Datenschutzbehörde, die Garante per la protezione dei dati personali, hat bei der Social-Media-App Clubhouse eine ganze Palette an Verletzungen der Privatsphäre der Nutzer festgestellt und dem US-Anbieter der Audiochat-App Alpha Exploration ein Bußgeld in Höhe von 2 Millionen Euro auferlegt. Clubhouse hatte sich vor allem während der ersten Phase der Corona-Pandemie als Online-Treffpunkt für den Austausch von Sprachnachrichten beliebt gemacht. Der anfängliche Hype rund um die App erlosch aber bald wieder.

Die Garante stellte bei ihren 2021 aufgenommenen Untersuchungen nach eigenen Angaben „zahlreiche Verstöße“ gegen die Datenschutz-Grundverordnung (DSGVO) bei Clubhouse fest. Diese reichen von mangelnder Transparenz bei der Verwendung der Daten von Nutzern und ihren „Freunden“ über die Möglichkeit für User Audionachrichten ohne die Zustimmung der registrierten Personen zu speichern und weiterzugeben, bis zur Profilerstellung und Weitergabe von Kontoinformationen ohne Angabe einer angemessenen Rechtsgrundlage. Zudem moniert die Aufsichtsinstanz „unbefristete Aufbewahrungsfristen“ für die von dem Betreiber des sozialen Netzwerks erstellten Aufzeichnungen. Alpha Exploration hatte diese damit begründet etwaigen Missbräuchen begegnen zu wollen. Die Garante untersagte dem Unternehmen zudem jede weitere Verarbeitung gesammelter Daten zu Marketing- und Profilingzwecken ohne ausdrückliche Zustimmung der Betroffenen. Die App hatte 2021 über 16 Millionen Nutzende weltweit und etwa 90.000 in Italien.

Ergänzend ordneten die Kontrolleure eine Reihe von Auflagen für den weiteren Clubhouse-Betrieb an. So muss Alpha Exploration die Nutzerinnen und Nutzer genauer darüber informieren, auf welcher Rechtsbasis Daten verarbeitet werden, und welche Speicherfristen für personenbezogene Informationen und Audiodateien gelten. Die Firma muss zudem einen klar ersichtlichen Rechtsvertreter im Einklang mit der DSGVO für EU-Bürger angeben. Die Garante hat Alpha Exploration ferner dazu verpflichtet eine Datenschutz-Folgenabschätzung für die über die Clubhouse-Plattform durchgeführte Datenverarbeitung durchzuführen.

Auch deutsche Datenschutzaufsichtsbehörden nahmen die Anwendung frühzeitig in den Blick. Sie sahen vor allem das Auslesen von Adressbüchern sowie Audiomitschnitte skeptisch. Die Hamburgische Datenschutzbehörde nahm im Februar 2021 Ermittlungen gegen Alpha Exploration auf. Ein Sprecher teilte mit, dass es zuletzt 2021 ein Gespräch mit einer von Clubhouse beauftragten Kanzlei gegeben habe. Diese habe dabei versichert, dass die Datenschutzerklärung von Clubhouse noch DSGVO-konform überarbeitet und ein europäischer Ansprechpartner benannt werde. Dieser Vertreter sitze inzwischen in Irland. Da es aber weiterhin keine Niederlassung der Betreiberfirma in der EU gebe, bleibe jede Datenschutzaufsichtsbehörde in Europa in ihrem Bereich zuständig. Vonseiten anderer deutscher Aufsichtsbehörden seien aktuell keine weiteren Aktivitäten oder Ermittlungen bekannt. Die französische Aufsichtsbehörde CNIL fühlt dem Unternehmen noch auf den Zahn. Die Anwendung sorgte auch wegen Sicherheitslücken und Datentransfers nach China für Schlagzeilen (Krempl, Clubhouse: Datenschützer verhängen Millionen-Strafe gegen Talk-App, www.heise.de 05.12.2022, Kurzlink: https://heise.de/-7366958).

Großbritannien

MI5 unterliegt Bürgerrechtsorganisationen wegen Datenspeicherung

Auf die Klage der Bürgerrechtsorganisationen Liberty und Privacy International (PI) hat das Investigatory Powers Tribunal (IPT), das für die Kontrolle der britischen Sicherheitsbehörden zuständig ist, mit Datum vom 30.01.2023 gerichtlich festgestellt, dass der britische Inlandsgeheimdienst MI5 zwischen 2014 und 2019 wissentlich große Mengen personenbezogener Kommunikationsdaten rechtswidrig gespeichert hat. Die Anfor-

derungen an die ordnungsgemäße Aufbewahrung, Überprüfung und Löschung wurden verletzt. Die Systeme hätten eine automatische Löschung nach der gesetzlich erlaubten Speicherfrist vorsehen müssen, was aber nicht der Fall war. Von dieser Praxis dürften Millionen Menschen betroffen gewesen sein.

Gemäß dem Urteil auf die 2020 eingereichte Klage gab es schon seit 2014 auf höchster Ebene des MI5 „sehr schwerwiegende Versäumnisse" beim Einhalten der Datenschutzbestimmungen. Mehrere aufeinanderfolgende britische Innenminister hätten diese langjährigen Regelverstöße trotz offensichtlicher Warnsignale nicht untersucht oder behoben. Die vom Innenressort ausgestellten Überwachungsanordnungen waren demnach unrechtmäßig. Sie erfüllten nicht die Schutzanforderungen aus den ohnehin wenig datenschutzfreundlichen Regulation of Investigatory Powers Act von 2000 (RIPA) und Investigatory Powers Act von 2016 (IPA).

Der MI5 hatte laut dem Urteil pflichtwidrig das Innenministerium nicht „vollständig und offen" bei Anträgen zur Durchführung von Überwachungsmaßnahmen über potenzielle Vorbehalte informiert. Er habe erst 2016 – also mit rund drei Jahren Verspätung – eingeräumt sich „eines sehr hohen Risikos bewusst" gewesen zu sein gegen die gesetzlichen Auflagen zu verstoßen. Das Innenressort versäumte es seiner Rolle als Aufsichtsinstanz gerecht zu werden. Da die Anordnungen, auf deren Basis der MI5 in das Recht auf Privatsphäre eingriff und massenhaft teils sensible persönliche Daten sammelte, nicht im Einklang mit dem Gesetz standen, verstießen sie auch gegen Artikel 8 der Europäischen Menschenrechtskonvention.

Megan Goulding, Anwältin bei Liberty, meinte, das Urteil zeige, „dass die sogenannten Sicherheitsvorkehrungen völlig unwirksam sind, wenn es darum geht unsere Rechte zu schützen und die Machthaber zur Rechenschaft zu ziehen." Die Regierung müsse nun rasch Einschränkungen schaffen, die die Privatsphäre der Bürger tatsächlich schützen. Die juristische Leiterin bei PI, Caroline Wilson Palow, ergänzte, es sei undemokratisch und gefährlich „dem MI5 einen Freifahrtschein zu geben". Die Bürgerrechtler hoffen, dass das IPT angesichts der erkannten Verstöße ein anderes Verfahren wieder eröffnet, in dem sie gegen die Massenüberwachungsbefugnisse des MI5 klagten. Auch dort habe der Geheimdienst Beweise nicht offengelegt, obwohl er dazu verpflichtet gewesen wäre (Krempl, Britischer Geheimdienst MI5 hat massenhaft Daten rechtswidrig gespeichert, www.heise.de 30.01.2023, Kurzlink: https://heise.de/-7476520).

Israel

„Toka" liefert manipulierende Überwachungstechnologie

Die Technik der israelischen Startup-Firma Toka ermöglicht es auf vernetzte Videokameras zuzugreifen und Übertragungen live oder im Nachgang zu verändern, was dazu führen kann, dass der Beweiswert von Videomaterial verloren geht. Toka ermöglicht es Sicherheitskameras und Webcams in einem bestimmten Umkreis zu lokalisieren, sie zu hacken und Übertragungen nicht nur zu verfolgen, sondern zu verändern. Gemäß einem israelischen Pressebericht ist es mit der Software von Toka möglich frühere Aufzeichnungen auszulesen. Ein „Zielgebiet" lasse sich überwachen, Kamera-Feeds könnten gestreamt und gesteuert werden. Die Anwendung befähige Nutzer auch dazu Autos ins Visier zu nehmen, um per Funk Zugang zu erhalten und „Fahrzeugforensik und -intelligenz" zu betreiben, also etwa den Kfz-Standort zu ermitteln.

Toka bündelt ausgewerteten Dokumenten zufolge diverse Dienste. Kunden seien so in der Lage visuelle Informationen aus „Live- oder aufgezeichneten Videos" zu sammeln. Sie könnten zudem Feeds von „Audio- und visuellen" Aufnahmen manipulieren, um etwa bei verdeckten Operationen „Aktivitäten vor Ort zu verschleiern". Den Israelis geht es dabei u.a. darum die Scharte auszuwetzen, dass die Polizei in Dubai nach dem Mord an einem Hamas-Kontaktmann 2010 stundenlanges Videomaterial aus einer Kamera zusammensetzen und 30 Mossad-Attentäter enthüllen konnte.

Das Unternehmen gründete der israelische Ex-Premierminister Ehud Barak 2018 zusammen mit dem früheren Cyberchef der israelischen Streitkräfte, General a.D. Yaron Rosen. Die zwei zusätzlichen Geschäftsführer Alon Kantor und Kfir Waldman stammen aus dem Bereich Cyberverteidigung. Wagniskapital kommt unter anderem von der US-Firma Andreessen Horowitz, an der das Internet-Urgestein Marc Andreessen beteiligt ist. Angeblich werden die Tätigkeiten von Toka durch das israelische Verteidigungsministerium streng reguliert.

Die Firma profiliert sich neben anderen israelischen Spyware-Exporteuren wie der NSO Group oder Candiru. Sie unterhält Büros in Tel Aviv und Washington und soll ausschließlich mit staatlichen Kunden in Regierungen, Geheimdiensten und Strafverfolgungsbehörden vor allem im Westen zusammenarbeiten und auch bereits Kontakte nach Deutschland geknüpft haben. Allein mit Israel bestehen dem Bericht nach seit 2021 Verträge im Wert von 6 Millionen US-Dollar; eine „Ausweitung des bestehenden Einsatzes" sei geplant.

Toka reklamiert für sich selbst „bisher unerreichbare Fähigkeiten", die ungenutzte Sensoren im notorisch unsicheren Internet of Things (IoT) „in Informationsquellen umwandeln" und diese so „für nachrichtendienstliche und operative Zwecke" genutzt werden können. Donncha Ó Cearbhaill aus dem Security Lab von Amnesty International in Berlin erklärte, dass vor allem Bluetooth- und WLAN-Schnittstellen oft Softwarefehler enthielten, die IoT-Geräte zu einem gefundenen Fressen für Hacker machten. Seien die Angreifer erst einmal in ein Netzwerk eingedrungen, könnten sie sich darin ausbreiten. Selbst eine „smarte" Glühbirne reiche aus, um ein WLAN-Passwort zu ergattern.

Der israelische Menschenrechtsanwalt Alon Sapir nannte die „Fähigkeiten, die früher unvorstellbar waren ... eine dystopische Technologie", die ernste Fragen aufwerfe. So könnten Videos manipuliert werden, „um unschuldige Bürger zu belasten oder dem System nahestehende Schuldige zu schützen". In Rechtsstaaten seien solche fingierten Aufzeichnungen nicht gerichtsfest (Krempl, „Dystopische Technologie": Startup hackt und manipuliert Überwachungskameras, www.heise.de 30.12.2022, Kurzlink: https://heise.de/-7444676).

USA

400-Mio. Dollar Strafe für Google wegen Werbeortung

Google sammelte jahrelang die Aufenthaltsdaten von Betroffenen für Werbezwecke, obwohl diese die Speicherung der Aufenthaltsorte ihres Android-Handys sowie iPhones mit Google Maps („Location History“) deaktiviert hatten. 2018 deckte dies der Journalist Ryan Nakashima von der Associated Press (AP) auf. Einige US-Staaten verklagten Google. Eine Gruppe von 40 Staaten setzte auf außergerichtliche Verhandlungen. Ihr Ergebnis ist eine Vergleichszahlung von 391,5 Millionen US-Dollar (rund 378 Millionen Euro).

Geleitet wurden die Untersuchungen und Verhandlungen von den Justizministern Nebraskas, Doug Peterson (Republikaner), und Oregons, Ellen Rosenblum (Demokratin). Für die ist der Vergleich „historisch“. Es sei der „größte, von US-Justizministern angeführte Vergleich im Bereich Verbraucherdatenschutz der Geschichte“. Die Vereinigten Staaten von Amerika haben bisher kein umfassendes Datenschutzgesetz. Es gibt lediglich Spezialgesetze z.B. für die Daten Minderjähriger oder Gesundheitsdaten. Die auf 40 Staaten aufgeteilten 400 Millionen Dollar sind nicht unbedingt viel: 2020 hat Arizona geklagt (Arizona v. Google, Arizona Sup. Ct., Az. CV2020-006219) und allein für sich die Einstellung der Datenschutzklage im Oktober 2022 von Google mit 85 Millionen Dollar abgelten lassen, also annähernd zwölf Dollar je Einwohner.

Der Vergleich mit den 40 Staaten kommt das Unternehmen vergleichsweise billiger. Oregon gibt an, 14,8 Millionen Dollar zu erhalten, auf Nebraska entfallen 11,9 Millionen. Das entspricht knapp 3,50 Dollar respektive 5,95 Dollar je Einwohner. Diese Summen fallen aber nur deshalb so „hoch“ aus, weil Nebraska und Oregon den Aufwand für Untersuchung und Verhandlungen abgegolten erhalten. Maryland beispielsweise erhält gerade einmal 1,40 Dollar je Einwohner.

In dem Vergleich verpflichtet sich Google dazu bei Aus- oder Einschaltung der Location History zusätzliche Informationen anzuzeigen, wichtige Information nicht zu verstecken und Nutzern jedenfalls anzuzeigen sowie generell mehr Auskunft über die Arten der Aufenthaltsdaten, die es sammelt, zu veröffentlichen. Kern des Problems ist, dass die Abschaltung der Location History alleine nicht reichte. Nutzer sollten auch die „Web & App Activity“ deaktivieren. Denn auch diese Daten erlauben es Google wertvolle Bewegungsprofile zusammenzustellen. Nicht mit von der Vergleichspartie sind unter anderem Indiana, Texas, Washington und der Hauptstadtbezirk District of Columbia. Diese vier Staaten haben Anfang des Jahres Klagen gegen Google erhoben (Sokolov, Google muss für Ortungs-Schwindel nicht einmal 400 Millionen zahlen, www.heise.de 1411.2022, Kurzlink: https://heise.de/-7340069).

USA

Gesichtserkennung bringt Mann fälschlich ins Gefängnis

Im US-Bundesstaat Georgia war der 28-jährige Randal Reid im November 2022 eine Woche lang inhaftiert, weil er per Gesichtserkennung mit einem Dieb zwei Bundesstaaten entfernt verwechselt wurde. Gemäß den Angaben seines Anwalts Tommy Calogero wurde der Schwarze auf der Fahrt mit seiner Mutter zum Thanksgiving-Essen in Georgia herausgewunken und darüber informiert, dass gegen ihn ein Haftbefehl der Gemeinde Jefferson Parish in Louisiana vorliege. Vom 25.11. bis zum 01.12. sei er dann im Gefängnis gewesen. Dann hätten die Verantwortlichen in Louisiana eingestanden, dass er nicht der Gesuchte sei. In den USA ist es nicht der erste derartige Fehler.

Gemäß dem Bericht wurde die Gesichtserkennung bei den Ermittlungen zum Diebstahl von wertvollen Designertaschen der Luxusmarken Chanel und Louis Vuitton im Wert von 10.000 US-Dollar eingesetzt.

Welche Software eingesetzt wurde, geht daraus nicht hervor. Die Polizei in dem Bundesstaat nutzte in der Vergangenheit offenbar Produkte des französischen Unternehmens Idemia und der Firma Clearview AI. Jedenfalls spuckte die Software den Namen des Mannes in Georgia aus, obwohl die Ähnlichkeit gering war: So sei dieser etwa 20 kg leichter als der von den Überwachungskameras aufgezeichnete Dieb und habe außerdem ein markantes Muttermal im Gesicht, das dem Dieb fehlt. Vor allem habe der aber „schwabbelige“ Arme gehabt, der Festgenommene nicht. Der sagte: „Ich war noch nie in meinem Leben in Louisiana und ich stehle auch nicht.“ Der Fehler sei schließlich „stillschweigend“ eingestanden worden, so das Zitat über den Anwalt: „Ich denke, sie haben gemerkt, dass sie sich mit der Festnahme auf Basis meines Gesichts zu weit aus dem Fenster gelehnt haben.“ Die Polizeibehörden hätten sich zu dem Vorfall nicht geäußert. Offenbar setzen viele Polizeibehörden nach einer Zurückdrängung von Gesichtserkennungstechnik wieder stärker darauf, weil die Zahl der Straftaten gestiegen ist. In New Orleans müssten alle potenziellen Funde eigentlich überprüft werden, es ist unbekannt, ob das hier geschehen ist.

Der Fall zeigt die mit der Technik verbundenen Risiken. Es ist nicht das erste Mal, dass jemand wegen eines fälschlichen Treffers im Gefängnis landet. Anfang 2020 musste in New York ein Mann 30 Stunden in Haft verbringen, bevor er gegen Kaution zu seiner Familie konnte. Es folgten weitere Fälle; immer waren schwarze Menschen betroffen. Auch deshalb wird oft darauf hingewiesen, dass die benutzten Algorithmen zur Gesichtserkennung bei ihnen schlechter funktionieren und deshalb Diskriminierung verfestigen können (Holland, Fehler bei Gesichtserkennung: Mann sitzt in den USA eine Woche im Gefängnis, www.heise.de 05.01.2023, Kurzlink: https://heise.de/-7449887; Schwarzer wegen Softwarefehler offenbar fast eine Woche inhaftiert, www.spiegel.de 05.01.2023).

USA

No-Fly-Liste als Zufallsfund

Nach den Terroranschlägen vom 11.09.2001 führte das „Terrorist Screening Center“ der US-Bundespolizeibehörde FBI zentrale Listen von Personen ein, die als Sicherheitsrisiko oder Terrorverdächtige eingeschätzt werden.

Diese Personen müssen bei jedem Flug eine erweiterte Sicherheitskontrolle erdulden oder dürfen das Flugzeug gar nicht erst betreten. Eine solche geheime Liste ist der Schweizer Hackerin „Maia Arson Crimew", die unter anderem an dem Verkada-Hack beteiligt war, in die Hände gefallen, die sie unter dem Namen „Nofly.csv" auf einem ungesicherten Testserver der US-Fluggesellschaft CommuteAir mit einem Umfang von 80 MByte fand. Die Liste enthält rund 1,5 Millionen Namen, überwiegend aus dem arabischen oder nahöstlichen Umfeld; es finden sich auch zahlreiche slawisch und spanische klingende Namen darunter. Mutmaßliche Mitglieder der nordirischen Terrorgruppe IRA sollen ebenfalls auf der Liste stehen.

Die Hackerin geht davon aus, dass es sich um die authentische Flugverbotsliste handelt. Die Daten stammen aus dem Jahr 2019 und wurden von der betroffenen Fluggesellschaft CommuteAir geschwärzt und enthalten nur Namen und Geburtsdaten der Personen.

Die Fluggesellschaft bestätigte den Zwischenfall und nahm den Server noch vor der Veröffentlichung offline. CommuteAir informierte die für den Flugverkehr zuständige Sicherheitsbehörde, die Transportation Security Administration. Die Hackerin berichtete auf ihrem Blog, dass sie aus Langeweile mit der Computer-Suchmaschine Zoomeye herumgestöbert habe und dabei auf den ungesicherten Testserver von CommuteAir gestoßen sei, auf dem die Automation-Software Jenkins lief. Nachrichten des Aircraft Communications Addressing and Reporting System (ACARS) hätten ihr Interesse geweckt, sodass sie genauer nachgeforscht habe was auf dem Server zu finden sei. Neben Anmeldeinformationen zu diversen Amazon-AWS-Instanzen der Fluglinie fand Crimew auf dem Server auch mehrere Namenslisten: employee_information.csv, nofly.csv und selectee.csv. Bei Letzterer handelt es sich laut der Hackerin um eine Liste von Personen, die bei jedem Flug umfangreiche Sicherheitskontrollen erdulden müssen.

Crimew teilte mit, dass sie die Daten Personenkreisen zugänglich macht, die ein berechtigtes Interesse daran hätten. Ihr sei bewusst, dass die Listen vertrauliche Informationen enthalten, sie glaube jedoch, dass es „in öffentlichem Interesse liegt diese Liste Journalisten und Menschenrechtsorganisationen zur Verfügung zu stellen". Im August 2021 hatte der ukrainische Sicherheitsforscher Wolodymyr Djatschenko ebenfalls eine – vermutlich sogar aktuellere – Liste von Personen gefunden, die die USA als Sicherheitsrisiko einstufen. Damals war eine Datenbank für jedermann frei auf einem Elasticsearch-Cluster mit bahrainischer IP-Adresse zugänglich und enthielt nicht nur die Namen von 1,9 Millionen Personen, sondern unter anderem auch deren Staatsbürgerschaft, Geschlecht, Geburtsdatum, die Reisepassnummer und den „No Fly"-Status.

Der Umfang der „No Fly"-Liste hat massiv zugenommen. Im Jahr 2006 sollen sich lediglich 44.000 Menschen darauf befunden haben. Die USA haben aber nicht nur gegen Einzelpersonen Flug- und Einreiseverbote verhängt: Die Trump-Regierung hatte 2017 aus Gründen der „nationalen Sicherheit" mehrheitlich den Einwohnern muslimischer Staaten sowie Nordkoreas und Venezuelas die Einreise in die USA untersagt (Zota, Hackerin findet „No Fly List" der US-Regierung auf Testserver einer Fluglinie, www.heise.de 22.01.2023, Kurzlink: https://heise.de/-7467140).

USA

Gesichtserkennung verhindert Musical-Besuch

Eine Rechtsanwältin in New York wurde per Gesichtserkennung identifiziert und aus einem Musical geworfen. Die Generalstaatsanwältin Letitia James hat wegen dieses Vorgangs der Madison Square Garden Entertainment Corporation (MSG) eine Reihe von Fragen gestellt, weil die Praxis gegen lokale und bundesweite Gesetze verstoßen haben könnte. Niemand dürfe bei bestimmten geschützten Aktivitäten diskriminiert werden; auch Vergeltung sei untersagt. MSG verteidigte sein Vorgehen und wies die Vorwürfe zurück.

Die Anwältin wollte Ende 2022 mit ihrer neunjährigen Tochter ein Weihnachtsmusical besuchen, das in der Radio City Music Hall im New Yorker Stadtteil Manhattan aufgeführt wurde, die von MSG geleitet wird. Deren Chef hatte zuvor ein Hausverbot für alle gegen das Unternehmen prozessierenden Anwaltskanzleien erteilt. Betroffen sind auch Anwälte und Anwältinnen, die nicht mit den Fällen betraut sind. Das Hausverbot bezieht sich auf alle Veranstaltungsorte. Die 44-jährige Frau war per Gesichtserkennungssoftware identifiziert und dann am Betreten der Veranstaltung gehindert worden. Gegen MSG hat sie angeblich nie prozessiert.

MSG widerspricht der Darstellung der Vorkommnisse nicht und versichert, dass es bei dem Vorgehen nicht darum gehe jemanden davon abzuhalten gegnerische Parteien vor Gericht zu vertreten: „Wir schließen lediglich einen kleinen Prozentsatz von Anwälten und Anwältinnen aus, während die Gerichtsverfahren laufen." Ob sich die Generalstaatsanwaltschaft davon überzeugen lässt, ist offen. Generalanwältin James meinte: „MSG Entertainment kann seine rechtlichen Schlachten nicht in den eigenen Arenen ausfechten." Jeder und jede mit Ticket müsse eingelassen werden und dürfe nicht wegen seiner Erscheinung ausgeschlossen werden. Sie fordert MSG auf die Praxis zu ändern (Holland, Per Gesichtserkennung identifiziert: Rauswurf aus Musical könnte Nachspiel haben, www.heise.de 27.01.2023, Kurzlink: https://heise.de/-7473472).

USA

Unternehmen vermeiden gezielt Aufmerksamkeit für Verlust sensibler Daten

Eine Studie von Jens Förderer, Professor für Innovation und Digitalisierung an der Technischen Universität München (TUM), und Sebastian Schütz, Professor für Wirtschaftsinformatik der Florida International University, zeigt am Beispiel von börsennotierten US-Firmen, dass Unternehmen Datenlecks bevorzugt an Tagen melden, an denen andere Nachrichten die Schlagzeilen in den Medien dominieren. Damit vermeiden sie stärkere Kursverluste am Aktienmarkt und riskieren größere Schäden bei den Betroffenen.

Jedes Jahr gelangen Unbefugte durch Hacking oder Datenpannen von Unternehmen an persönliche Informationen von Millionen Menschen, etwa an Passwörter, Kreditkartendaten oder Gesundheitsinformationen. Die Folgen für die Betroffenen können verheerend sein, von finanziellen Schäden bis hin zu Identitätsdiebstahl. Um ihre Kunden davor zu schützen, sind Firmen in vielen Ländern, so auch in den USA, gesetzlich verpflichtet den Vorgang den Aufsichtsbehörden zu melden und die Kunden zu informieren, wodurch die Lecks meist auch öffentlich werden.

In solchen Situationen ist eigentlich Eile geboten, um eine Verbreitung und möglichen Missbrauch der Daten einzudämmen. Allerdings bieten Gesetze den Unternehmen zeitliche Freiräume. In der EU muss jedes Datenleck, das zu einem Risiko für betroffene Personen führen kann, innerhalb von 72 Stunden gemeldet werden. In den USA variieren die Meldefristen je nach Bundesstaat zwischen 30 und 90 Tagen.

Als sich die Wissenschaftler mit solchen Vorfällen beschäftigten, wunderten sie sich, dass die Veröffentlichung der Datenverluste relativ geringe Folgen für den Aktienkurs der Unternehmen hatte, so Jens Förderer: „Das hat uns überrascht, da Datenlecks für die Firmen ja einen Imageverlust und ein sinkendes Kund:innen-Vertrauen bedeuten, was ihren Wert am Aktienmarkt eigentlich stark belasten sollte. Unsere Hypothese war, dass die Aufmerksamkeit der Anleger:innen abgelenkt war."

Die Forscher identifizierten den Zeitpunkt der Veröffentlichung von mehr als 8.000 Datenlecks börsennotierter US-amerikanischer Unternehmen zwischen 2008 und 2018, wobei sie Informationen der Non-Profit-Organisation Identity Theft Ressource Center (ITRC) nutzten. Dann glichen sie die Zeitpunkte mit Tagen ab, an denen viele Firmen ihre Quartalszahlen vorstellten – also Tagen, von denen im Voraus klar war, dass eine Vielzahl an marktrelevanten Informationen publik werden würde. Dafür werteten sie das „Wall Street Journal" aus, die größte Wirtschaftszeitung der USA.

Die Studie bestätigte, dass an Tagen, an denen andere Meldungen die Schlagzeilen dominierten, signifikant mehr Datenlecks veröffentlicht wurden. Besonders deutlich war der Zusammenhang zwischen Nachrichtenlage und Veröffentlichungstag bei schwerwiegenden Datenverlusten, bei Pannen mit Firmen-internen Ursachen und wenn Gesundheitsinformationen oder Ausweisdaten betroffen waren: „An hektischen Tagen müssen sowohl Redaktionen als auch Analyst:innen Prioritäten setzen, welche Informationen sie aufgreifen. Unsere Ergebnisse legen nahe, dass Unternehmen die Bekanntgabe ihrer Datenlecks strategisch planen und gezielt auf eine geringere Aufmerksamkeit setzen."

Die Forscher wollten zudem wissen, ob das Kalkül der Unternehmen aufgeht. Dafür untersuchten sie die Aktienkurse der Firmen nach der Bekanntgabe der Datenverluste. Sie stellten fest, dass die Unternehmen im Durchschnitt einen Kursverlust verzeichnen mussten, der aber an Nachrichten-starken Tagen deutlich geringer ausfiel, so Sebastian Schütz: „Unternehmen, die ihre Fehler im Umgang mit Daten im Schatten anderer Ereignisse verstecken, vermeiden so auch den öffentlichen Druck, dass sie selbst und andere Firmen stärkere Maßnahmen gegen Datenlecks ergreifen müssen."

Jens Förderer empfiehlt die Spielräume für die Bekanntgabe von Datenverlusten möglichst eng zu fassen: „Je länger die Meldefrist für einen Datenverlust ist, desto eher können Unternehmen die Bekanntgabe strategisch planen und den Zweck der Bekanntgabe unterlaufen" (Technische Universität München, PM 24.11.2022, Firmen melden Datenlecks an Nachrichten-starken Tagen).

USA/China

TikTok überwacht Journalisten

Das chinesische Unternehmen Bytedance hat seine Video-App TikTok dazu missbraucht die Bewegungen mehrerer US-Journalisten und ihrer Angehörigen zu überwachen, die die App auf ihren Handys installiert hatten. Einen früheren Bericht darüber hatte das chinesische Unternehmen in Abrede gestellt. Ende 2022 sprach dann Bytedance-Chef Liang Rubo vom „Fehlverhalten einiger weniger Einzelpersonen", das wohl „eine Lehre für uns alle" sein werde. Die Überwachung der kritischen Journalisten erfolgte unter dem internen Codenamen Project Raven. Betroffen sind laut einer internen Untersuchung im Auftrag Bytedance' jedenfalls die Forbes-Journalisten Emily Baker-White, Katharine Schwab und Richard Nieva, die früher bei Buzzfeed News gearbeitet haben. Außerdem sollen ein Financial-Times-Journalist sowie ein nicht namentlich genannter ehemaliger Buzzfeed-Mitarbeiter sowie Angehörige dieser Personen überwacht worden sein.

Bytedance/TikTok-Mitarbeiter sollen wiederholt die Aufenthaltsdaten aus den App-Logs abgerufen haben. Damit wollten sie wohl herausfinden, ob die Überwachten mit Bytedance-Mitarbeitern Kontakt haben. Einer oder mehrere Mitarbeiter hatten Beweise für unlautere Machenschaften bei TikTok an Buzzfeed weitergegeben: Tonaufnahmen von 80 internen Besprechungen belegen, dass aus China wiederholt auf die Daten von US-amerikanischen TikTok-Nutzern zugegriffen wurde.

Dieser Missbrauch personenbezogener Daten ist Wasser auf die Mühlen jener, die TikTok als Risiko für die nationale Sicherheit der USA einstufen und auf ein Verbot der App dringen. In 19 US-Staaten ist die TikTok-App auf Diensthandys von Beamten bereits verboten oder blockiert. TikTok gilt als derzeit meistbesuchtes Online-Angebot der Welt. Schon vor mehr als zwei Jahren hat Chinas Nachbar Indien über 200 chinesische Apps gesperrt, darunter TikTok, Alipay und WeChat.

Der demokratische US-Senator Mark Warner, Vorsitzender des Geheimdienstausschusses, drohte mit einem TikTok-Verbot in den USA: „Diese neue Entwicklung verstärkt schwere Bedenken, dass das soziale Netzwerk (Mitarbeitern) in der Volksrepublik China erlaubt hat wiederholt auf private Daten von US-Nutzern zuzugreifen, entgegen wiederholter Beteuerungen, dass diese Daten geschützt waren. Das Justizministerium verspricht seit mehr als einem Jahr, dass sie nach Wegen suchen US-Nutzer vor Bytedance und der Kommunistischen Partei Chinas zu schützen. Es ist an der

Zeit eine Lösung zu präsentieren, oder das Parlament wird bald gezwungen sein einzugreifen."

Für die rechtswidrige Überwachung macht Bytedance offenbar ausgerechnet jene Mitarbeiter verantwortlich, die die Einhaltung von Vorschriften überwachen sollten. Chris Lepitak, Leiter der internen Revision, wurde gefeuert, außerdem je ein weiterer Mitarbeiter in den USA und in der Volksrepublik China. Lepitaks chinesischer Chef Song Ye, der direkt Konzernchef Rubo Liang untersteht, hat laut Forbes selbst den Hut genommen. Project Raven soll aus China genehmigt worden sein; ausgerechnet der Datenschutzbeauftragte TikToks, zugleich Sicherheitschef, soll sich daran beteiligt haben. Zudem soll der Leiter der weltweiten Legal Compliance eingeweiht gewesen sein. TikTok-Sprecherin Hilary McQuaide hat Forbes versichert, dass keiner der Übeltäter mehr für den Konzern arbeite. Weitere Details zu Konsequenzen für (Ex-)Mitarbeiter gibt das Unternehmen nicht preis (Sokolov, TikTok überwacht Journalisten per App, www.heise.de 23.12.2022. Kurzlink: https://heise.de/-7441812).

Taiwan

Angebliches Promi-Hacking gegen China Airlines

Die taiwanische Fluggesellschaft China Airlines bestätigte anonyme Drohungen von Hackern erhalten zu haben. Offenbar um ihre Forderungen zu untermauern, haben die Angreifer eine Liste prominenter Personen aus Taiwan im Internet veröffentlicht. Allerdings würden die Daten nicht denen aus ihrem Vielfliegerprogramm („Dynasty Flyer") entsprechen, sodass unklar ist, ob diese Liste tatsächlich aus einem Cyberangriff stammt. Nachdem China Airlines nicht öffentlich zugab von Hackern angegriffen worden zu sein, wurden weitere Daten veröffentlicht. Die Liste enthält unter anderem den Gründer des Chipauftragsfertigers TSMC, Morris Chang, den taiwanischen Vizepräsidenten Lai Ching-te, den Außenminister Taiwans, Joseph Wu, und Prominenz aus der Unterhaltungsbranche des Landes.

China Airlines hat nach eigenen Angaben umgehend die Ermittlungsbehörden über die Drohungen informiert und untersucht die Sicherheit seines Systems. Mitglieder des Vielfliegerprogramms wurden daran erinnert ihre Passwörter regelmäßig zu ändern. Die Fluggesellschaft erklärte dennoch, dass die veröffentlichten Daten nicht zu den eigenen Informationen passen würden, sodass es unmöglich sei zu erkennen, welchen Ursprungs diese Daten seien. Die taiwanische Flugaufsichtsbehörde CAA (Civil Aeronautics Administration) fordert China Airlines auf die Angelegenheit umgehend zu erklären und einen Bericht vorzulegen, wie die Situation verbessert werden könnte und wie mit ähnlichen Vorfällen künftig umgegangen wird. Die Fluggesellschaft solle außerdem eine umfassende Sicherheitsuntersuchung ihrer Systeme durchführen.

China Airlines wurde 1959 in Taiwan gegründet und gehört zur Luftfahrtallianz SkyTeam, wie etwa auch die französische Air France und die US-amerikanische Delta Air Lines. Sie ist nicht zu verwechseln mit China Air der Volksrepublik China und bietet seit Jahren regelmäßige Direktflüge zwischen Deutschland und Taiwan an. Viele Jahre war dies exklusiv, erst seit Kurzem ist mit der taiwanischen EVA Air eine zweite Fluglinie mit Direktflügen nach Deutschland hinzugekommen (Schräer, Taiwanische Fluglinie untersucht möglichen Hacker-Angriff auf Passagierdaten, www.heise.de 16.01.2023, Kurzlink: https://heise.de/-7459645).

Australien

Nach Lösegeldverweigerung Daten von Medibank im Darknet

Einen Monat nach dem Cyberangriff auf den australischen Krankenversicherer Medibank tauchten dabei erbeutete Daten im Darknet auf. Es handelt sich um Namen, Adressen, Geburtstage, Telefonnummern, E-Mail-Adressen sowie teilweise Kundennummern, Ausweisnummern und einige Daten zu Gesundheitsleistungen. Insgesamt sollen 9,7 Millionen Menschen betroffen sein. Medibank rät ihren Kunden und Kundinnen bei jeglicher Online-Kommunikation und bei Transaktionen vorsichtig zu sein, die Daten könnten für betrügerische Zwecke benutzt werden. Australiens Bundespolizei zeigte sich beunruhigt, da es um sehr persönliche Daten gehe. Man habe Maßnahmen ergriffen und eine nach einem anderen Hackerangriff eingerichtete Initiative auf den Vorfall bei Medibank ausgeweitet. Das Unternehmen hatte sich geweigert ein Lösegeld für die Daten zu zahlen.

Medibank hat nach eigener Aussage mehr als 3,9 Millionen Kunden und Kundinnen in Australien; das Unternehmen vertreibt vor allem Krankenversicherungen. Betroffen sind auch ehemalige Kunden, Daten bei einer Tochterfirma und Kunden im Ausland, weshalb deutlich mehr Menschen als anfangs gedacht betroffen sein dürften.

Über einen „Cyber-Vorfall" hatte Medibank Mitte Oktober 2022 berichtet und eine „forensische Analyse" angekündigt. Sie hatte anfangs nicht mitgeteilt, ob und in welchem Umfang Daten abgegriffen wurden. Später hatten sich die mutmaßlichen Täter an das Unternehmen gewandt und erklärt, sie hätten 200 Gigabyte an sensiblen Daten erbeutet. Damit die nicht weitergegeben würden, müsse Medibank Geld zahlen. Außerdem wurde gedroht, dass prominente Kunden und Kundinnen kontaktiert und mit sensiblen Gesundheitsdaten konfrontiert würden, sollte kein Lösegeld fließen. Die Reaktion von Medibank: „Basierend auf den umfangreichen Ratschlägen, die wir von Experten für Cyberkriminalität erhalten haben, glauben wir, dass es nur eine begrenzte Chance gibt, dass die Zahlung eines Lösegelds die Rückgabe der Daten unserer Kunden sicherstellt und verhindert, dass sie veröffentlicht werden." Diese Vorgehensweise stimme mit den Empfehlungen der Regierung Australiens überein. Premierminister Anthony Albanese erklärte, er sei selbst Kunde bei Medibank: „Das ist wirklich hart für die Betroffenen." Aber das Unternehmen habe die Richtlinien befolgt. Seine Regierung will die Strafen für „wiederholte und ernsthafte" Datenschutzverstöße deutlich erhöhen (Holland, Lösegeld nicht bezahlt: Daten von australischem Krankenversicherer im Darknet, www.heise.de 09.11.2022, Kurzlink: https://heise.de/-7334201).

Brasilien

Crowd-Investigation gegen rechte Demonstranten

Nachdem rechtsradikale Aufständische am 08.01.2023 mehrere Regierungsgebäude und das Oberste Gericht in der brasilianischen Hauptstadt Brasilia verwüstet hatten, tauchte auf Instagram ein neuer Account auf. Unter dem Namen „Contragolpe Brasil" – ein Wortspiel, das sowohl „Gegen den Putsch in Brasilien" als auch „Gegenschlag Brasilien" bedeuten kann – wurden Fotos von mutmaßlichen Teilnehmern des Sturms gepostet. Die Idee, so die Macher hinter dem Account, sei Informationen zu sammeln, mit denen „Menschen, die die Demokratie in Brasilien angreifen wollen", identifiziert werden könnten. Damit wolle man es den Behörden einfacher machen Täter zu finden und zu bestrafen, die an diesem Tag einer Verhaftung entgangen seien.

Schon nach 24 Stunden erreichte der Account der Aktivisten 1,1 Millionen Follower. David Nemer, Professor für Medienwissenschaften an der Universität von Virginia, der auch Mitglied der Fakultät der Harvard University ist, kommentierte: „Ich bin überhaupt nicht überrascht, dass dieses Konto so schnell zustande kam. Wir alle wussten, dass sich [die Aufständischen] in WhatsApp-Gruppen und Telegram-Kanälen organisiert hatten, weil die alle offen waren. Das wurde alles in den sozialen Medien angekündigt. [Der Sturm] war also zu erwarten, es gab keine Geheimhaltung."

Diejenigen, die die Attacke durchgeführt haben, waren Anhänger des ehemaligen Präsidenten Jair Bolsonaro, der die Wahl gegen den linken Kandidaten Luis Inácio Lula da Silva zuvor verloren hatte. Aus Protest gegen die Wahl kampierten sie zunächst vor Militärkasernen im ganzen Land, bevor sie dann mit Bussen in die Hauptstadt Brasilia fuhren, um dort gewalttätig zu demonstrieren. Während die Angreifer auf dem Rasen der brasilianischen Bundesregierung und im brasilianischen Kongress, dem Obersten Gerichtshof Brasiliens sowie dem Präsidentenpalast randalierten, hinterließen sie Spuren in Form von Posts, Videos und Fotos. Sie teilten ihre Aktion sowohl auf öffentlichen Social-Media-Plattformen als auch in privaten Messaging-Apps. Viele Dutzend dieser Bilder wurden von „Contragolpe Brasil" gesammelt und mittlerweile veröffentlicht. Auf praktisch jedem Foto sind Gesichter von Menschen zu sehen.

Die Betreiber des Instagram-Accounts Contragolpe Brasil sind bislang anonym. Sie forderten Sympathisanten dazu auf auch private Nachrichten mit Fotos und Identifizierungsdaten einzuschicken. Sie baten zudem darum solche Informationen an die Behörden weiterzuleiten. Contragolpe Brasil ist nicht die einzige Crowdsourcing-Aktion, die in Brasilien zur Identifizierung der Täter des 08.01.2023 läuft. Agência Lupa, ein Team von Faktencheckern, hat eine Datenbank mit Text-, Foto- und Videobeiträgen vom Tag des Aufstands erstellt, deren Informationen sich aus anonymen (auch privaten) Quellen speisen.

Die Identifizierung von Teilnehmern gewalttätiger Veranstaltungen durch das Durchsuchen sozialer Medien findet nicht zum ersten Mal statt. Die Methode kam auch zur Identifizierung von Verantwortlichen für den Sturm auf das US-Kapitol in Washington am 06.01.2021 zum Einsatz. Manche der dabei aktiven Gruppen wie etwa die sogenannten Deep State Dogs gingen dabei bis ins Detail und schauten sich genaue Taten wie Sachbeschädigung oder den Angriff der Presse näher an.

In Brasilien entwickelt sich eine ähnliche Dynamik. Nicht lange nachdem Contragolpe Brasil mit den Veröffentlichungen begonnen hatte, trudelten die ersten Kommentare ein. In einem wurde ein möglicher Name für einen „bärtigen Mann mit dunkler Sonnenbrille, einer Adidas-Baseballkappe und einem gelb-grünen Trikot der brasilianischen Fußballnationalmannschaft" genannt. Er sei ein Beamter im Bundesstaat Paraná, so der Kommentator. Jemand fragte daraufhin, für welche Behörde er arbeite, damit sie markiert werden könne und die Leute „angemessene Maßnahmen fordern" könnten. Dann hieß es, dass der Mann auf dem Foto bereits entlassen worden sei.

Inzwischen wurden die Bildunterschriften zu den auf Contragolpe Brasil veröffentlichten Fotos geändert. Einige enthielten die vollständigen Namen der Personen, ihre Wohnorte und die Bundesstaaten, in denen sie leben. Sogar Instagram-Accounts wurden aufgeführt. Mittlerweile gibt es eine Form von Selbstzensur. Der Versuch, Kriminelle online zu identifizieren, kann danebengehen, wenn die Bürger sich irren, wofür es Beispiele gibt. Eine Frau behauptete ein Hacking-Opfer zu sein, das entsprechende Bild sei nicht von ihr eingestellt worden. Mittlerweile ist sie untergetaucht.

Instagram reagierte. Es war eine gewisse Zeit nicht mehr möglich neue Beiträge auf Contragolpe Brasil zu posten. Wie es dazu kam, bleibt unklar; die Meta-Tochter antwortete zunächst nicht auf eine Pressenachfrage. Die Aktivisten reagierten damit ihre Inhalte über Instagram-Stories zu teilen. Eine davon verkündete einen Erfolg: die Verhaftung von Ana Priscila Azevedo, was auch die Strafvollzugsbehörde im Bundesdistrikt Brasiliens bestätigte. Azevedo war über den Dienst von Contragolpe Brasil identifiziert worden. Darin wird sie als eine „der Organisatorinnen des Aufstandes" bezeichnet. Insgesamt sollen 1.166 Personen zwischen dem 08.01. und dem 11.01. verhaftet worden sein, wie viele davon durch die „Unterstützung" von Social Media, ist unklar.

Es ist außerdem unklar, ob die Behörden Contragolpe Brasil bei ihren Ermittlungen gegen Azevedo oder andere Personen, die verhaftet wurden, tatsächlich genutzt haben. Das Ministerium für Justiz und öffentliche Sicherheit Brasiliens reagierte nicht auf eine Bitte um Stellungnahme. Medienwissenschaftler Nemer glaubt, es wäre ein Hilfsmittel gewesen: „Social-Media-Posts sind aber nur eine Art von Beweisen. Ich bin mir sicher, dass die Polizei allein durch die Namen dieser Leute noch mehr herausfinden könnte" (Langlois, Unruhen in Brasilien: Wie Aktivisten Aufständische über Instagram finden wollen, www.heise.de 18.01.2023, Kurzlink: https://heise.de/-7460855).

Technik-Nachrichten

Sicherheitsforscher entdecken viele Kfz-Datenlecks

Forscher haben verschiedene Komponenten von etlichen Automarken auf Sicherheit abgeklopft und sind auf unzählige wunde Punkte gestoßen. Sie konnten eigenen Angaben zufolge unter anderem auf interne Mitarbeiter-Daten von Autoherstellern zugreifen, Accounts von Kunden übernehmen und die komplette Kontrolle über einige Autos erlangen, nachdem sie Webportale und Programmierschnittstellen (APIs) analysierten und dabei Schwachstellen entdeckten.

Gemäß der Auflistung konnten sie Modelle von unter anderem Kia, Honda, Hyundai und Nissan öffnen und den Motor starten. Dafür benötigten sie eigenen Angaben zufolge lediglich die Fahrzeug-Identifikationsnummer (FIN), die sie in einer HTTP-Anfrage an den Endpoint schickten. Bei vielen Modellen kann man diese Nummer durch die Windschutzscheibe ablesen. Die Attacken gehen auf Schwachstellen in der SiriusXM-Plattform zurück, die weltweit bei rund 12 Millionen vernetzten Autos zum Einsatz kommen soll.

Aufgrund von unsicher konfigurierten Single-Sign-On-Schnittstellen in Händlerportalen konnten die Forscher eigenen Angaben zufolge unter anderem auf Github-Instanzen, interne Firmendaten, Mitarbeiter-Informationen und Kundendaten zugreifen. Das war etwa bei Ferrari, Mercedes-Benz, Porsche und Toyota der Fall. Aufgrund von Schwachstellen konnten sie z.B. über vergleichsweise simple HTTP-Anfragen Accounts von BMW-Mitarbeitern zurücksetzen, diese übernehmen und sich so Zugriff verschaffen. In Webportalen von Mercedes und Rolls-Royce konnten die Forscher sogar eigenen Code ausführen und hatten Zugriff auf hunderte interne Tools. Aus dem Bericht geht nicht hervor, ob die Autohersteller die Schwachstellen geschlossen haben; gemäß einem Tweet war dies zumindest bei Nissan Bugs der Fall (Schirrmacher, Geöffnet und weggefahren: Sicherheitsforscher knacken Autos von Kia, Honda & Co., www.heise.de 04.01.2023, Kurzlink: https://heise.de/-7447668).

Meta nutzt Biometrie zur Altersverifizierung

Facebook erprobt Möglichkeiten, wie Plattform-User ihr Alter bei der Nutzung von deren Dating-App verifizieren können. Dazu zählt auch ein KI-Gesichtsscan-Tool. Meta, Facebooks Mutterkonzern, hat bisher KI-Gesichtsscanner eingesetzt, um das Alter von Instagram-Nutzern zu verifizieren. Jetzt sagt das Unternehmen, dass es das Tool bei Facebook-Dating-Nutzern testen wird.

Meta kündigte am 05.12.2022 in einem Blogbeitrag an damit zu beginnen Nutzerinnen und Nutzer von Facebooks Dating-App aufzufordern ihr Alter zu verifizieren, wenn die Plattform vermutet, dass sie minderjährig sind. Um den Dating-Service zu nutzen gilt eine Altersgrenze von 18 Jahren. Meta wird bei Facebook Dating demnach die Altersverifizierungstechnologie des britischen Unternehmens Yoti einsetzen, das die Nutzenden auffordert ein Ausweisdokument hochzuladen oder die Yoti-Technologie zur Altersschätzung per Gesichtsscan zu verwenden. Meta teilt demnach ein Standbild aus dem Video-Selfie mit Yoti, das das Alter anhand der Gesichtszüge schätzt. Yoti könne die Identität nicht erkennen, so Meta. Das System wird zunächst für Nutzende in den USA eingeführt.

Erica Finkle, Direktorin für Data Governance des Unternehmens, erläuterte: „Indem wir den Menschen mehr als eine Option zur Verifizierung ihres Alters anbieten, können sie die Methode wählen, die am besten zu ihren Bedürfnissen und Vorlieben passt. Zum Beispiel haben viele Menschen nicht immer Zugang zu Ausweispapieren, die eine Altersverifizierung deutlich machen." Die neuen Altersüberprüfungssysteme sollen dazu beitragen Minderjährige davon abzuhalten auf Funktionen zuzugreifen, die für Erwachsene gedacht sind. Für Volljährige selbst scheint es keine Anforderungen zu geben ihr Alter auf Facebook Dating zu verifizieren, z.B. um sicherzustellen, dass ein 45-Jähriger sich nicht als 18-Jähriger ausgibt.

Meta hat Yoti zuvor schon eingesetzt, z.B. zur Altersüberprüfung von Instagram-Nutzenden, die versuchen ihr Geburtsdatum so zu ändern, dass sie 18 oder älter sind. Yoti behauptet, dass sein System im Großen und Ganzen sehr genau sei. Die Rate der korrekten Identifizierung von 13- bis 17-Jährigen als unter 23 Jahre alt betrage 99,65%. Meta sagt, dass die Altersverifizierung „Hunderttausende" von Menschen in altersgerechte Versionen der App sortiert hat und dass 81% der Nutzenden, die von Instagram aufgefordert werden ihr Alter zu verifizieren, die Selfie-Option von Yoti nutzten. Instagram betont, dass das System zur Altersverifikation von Yoti datenschutzfreundlich und vom Age Check Verification Scheme, einer britischen Non-Profit-Organisation, verifiziert sei. Auch würden laut Instagram verschiedene Jugend- und Datenschutzorganisationen das System von Yoti empfehlen, darunter etwa die deutsche Kommission für Jugendschutz (KJM).

Das System ist nicht für alle Menschen gleich genau: Die Daten von Yoti zeigen, dass die Genauigkeit bei „weiblichen" Gesichtern und Menschen mit dunklerer Hautfarbe schlechter ist, so die Zeitschrift „The Verge". Forscher haben zudem darauf hingewiesen, dass Gesichtserkennungs- und -analysesoftware generell bei Menschen unterschiedlichen Alters, Hautfarbe und Geschlechts verschieden gut funktioniert. So kam es vor, dass Facebooks Gesichtserkennung schwarze Menschen für Affen hielt. In einem News-Clip wurde Rassismus gegen Schwarze thematisiert; Facebooks KI schlug Nutzern dazu vor mehr „Videos über Primaten" anzuzeigen (Knobloch, Meta: KI-Gesichtsscans für Facebook Dating, www.heise.de 05.12.2022, Kurzlink: https://heise.de/-7367036).

Meta-Mitarbeitende bereicherten sich über exklusive kriminelle Dienstleistung

Gemäß einem Pressebericht hat der Facebook-Mutterkonzern Meta im Jahr 2022 mehr als zwei Dutzend Angestellte entlassen, deren Aufgabe es eigentlich war Nutzenden mit Log-in-Problemen zu helfen. Stattdessen seien die Accounts missbräuchlich übernommen worden. In einigen Fällen sollen Mitarbeitende mehrere Tausend US-Dollar Bestechungsgelder von Cyberkriminellen angenommen haben. Unter den Entlassenen seien sowohl Mitarbeiter als auch Auftragnehmer mit Zugang zu sicherheitsrelevanten internen Mechanismen gewesen. Dem Bericht zufolge seien die Personen in einer langwierigen internen Untersuchung identifiziert worden. Man werde, so wird ein Meta-Sprecher zitiert, weiterhin geeignete Maßnahmen gegen die Verstöße und die daran beteiligten Personen ergreifen.

Das intern „Oops“ (Online Operations) bezeichnete Programm existiert seit den frühen Jahren von Facebook und sollte für „Sonderfälle“ genutzt werden, die Probleme (vergessene Zugangsdaten oder gehackte Konten) mit ihren Accounts haben. Die Möglichkeit zur Nutzung des „Oops“-Programms sollte auf Mitarbeiter des Teams von CEO Mark Zuckerberg, Geschäftspartner, Familienmitglieder oder Persönlichkeiten des öffentlichen Lebens beschränkt sein, von deren Konten auch wirtschaftliche Erfolge abhängen. Das „Oops“-Team, das für Facebook- und Instagram-Konten zuständig ist, soll internen Dokumenten zufolge 2020 über 50.000 Anfragen bearbeitet haben, drei Jahre zuvor waren es demnach 22.000. In den „Oops“-Berichten angegebene E-Mail-Adressen zum Zurücksetzen des Passworts des jeweiligen Accounts seien an das Community-Support-Team von Meta weitergeleitet worden, sofern die automatische Funktion zum Zurücksetzen des Passworts nicht funktionierte oder Nutzer ihre E-Mail-Adressen vergessen hatten.

Um die Nutzenden, deren Geschäft in großen Teilen von sozialen Netzwerken abhängig ist, habe sich ein lukratives, kriminelles Geschäft entwickelt. Die kompromittierten Accounts seien in Online-Foren für Zehntausende Dollar verkauft worden. Sogenannte „Vermittler“ berechneten demnach – für die Rückgewinnung der Kontrolle – den eigentlichen Besitzern „eine entsprechende Gebühr“. Das sei gemäß dem Bericht nur möglich, weil die Kriminellen Zugang zu Mitarbeitern des Meta-Konzerns hätten und der reguläre Zugriff auf das „Oops“-Team dem größten Teil der mehr als drei Milliarden Nutzenden von Facebook und Instagram nicht zur Verfügung stehe. Den Kundenservice werde Meta eigenen Angabe zufolge in den kommenden Jahren ausbauen. 2017 gab Facebook bekannt mit Delegated Recovery den Passwort-Reset via E-Mail abzulösen (Mewes, Geschäft mit Benutzerkonten: Meta-Mitarbeiter verkaufen Zugangsinformationen, www.heise.de 18.11.2022, Kurzlink: https://heise.de/-7345337).

Twitter-Konto-Daten frei im Netz

Am Weihnachtswochenende 2022 wurde bekannt, dass in Untergrundforen eine Datenbank mit rund 400 Millionen Datensätzen von Twitter-Konten zum Verkauf stehe. Diese enthalte offenbar echte Daten wie E-Mail-Adressen oder öffentlich verfügbare Informationen. Die Datenbank wurde schließlich weitergegeben und ist mit 235 Millionen Einträgen seit Januar 2023 anscheinend frei verfügbar. Es besteht der Verdacht, dass die Datendiebe eine Mitte 2022 von Twitter bestätigte Schwachstelle missbraucht haben, um mittels „Scraping“ an die Nutzerdaten zu gelangen. Auf das ursprüngliche Untergrund-Foren-posting stieß zunächst der israelische Sicherheitsforscher Alon Gal.

Gal beobachtete den Vorfall weiter und veröffentlichte seine neuen Erkenntnisse in seinem LinkedIn-Profil. Er geht von der Echtheit der Datenbank aus. Inzwischen hätten mehr als ein Cyberkrimineller die Daten zum Verkauf angeboten. Er korrigierte jedoch seine Einschätzung, dass anstatt der ursprünglich angenommenen 400 Millionen Datensätze nur die von 235 Millionen Twitter-Nutzer enthalten seien; dies hätten zwei Verkäufer bekräftigt, die rund 190 Millionen Dubletten in dem Datenfundus ausgemacht hätten. Außerdem seien zwar private Informationen wie die E-Mail-Adresse sowie öffentliche Informationen enthalten, nicht jedoch die Telefonnummer. Der IT-Sicherheitsforscher ergänzte, dass die ursprünglich missbrauchte Lücke es ermöglichte Nutzer mittels ihrer Telefonnummer zu finden. Daher geht er davon aus, dass die Cyberkriminellen diese Funktion genutzt hätten und eine Datenbank mit Telefonnummern existiert. Belege liefert Gal dafür jedoch nicht.

Schließlich stellte Alon Gal fest, dass die Datenbank nach starkem Kursieren im Untergrund veröffentlicht wurde. Er schätzt, dass die Daten jetzt insbesondere für gezieltes Phishing missbraucht werden können. Twitter-Nutzende sind deshalb gut beraten Vorsicht bei vermeintlichen Nachrichten oder E-Mails von Twitter walten zu lassen. Es könnte sich um gut gemachtes Phishing handeln (Knop, Datenleck: Datenbank mit 235 Millionen Twitter-Konten kursiert, www.heise.de 05.01.2023, Kurzlink: https://heise.de/-7449391).

Rechtsprechung

EGMR

Auskunftsverweigerung hindert Gegendarstellungsanspruch nicht

Nach neun Jahren hat der Europäische Gerichtshof für Menschenrechte (EGMR) mit seinem Urteil vom 17.01.2023 einen Strich unter den Rechtsstreit zwischen der früheren Geschäftsführerin der Linksfraktion im Bundestag, Ruth Kampa, und dem Axel-Springer-Verlag und seiner Zeitung „Welt“ gezogen und deren Gegendarstellungspflicht bestätigt (Az. No. 8964/19). Der Umstand, dass Kampa der Welt zunächst eine Stellungnahme verweigert hatte, ändert an dieser Pflicht nichts. Im Oktober 2013 hatte die Zeitung Welt einen Artikel über „Die Stasi-Frau an Gysis Seite“ veröffentlicht. Gemeint war Kampa. Die Frau, deren langjährige Arbeit für die Stasi damals öffentlich gemacht wurde, galt dem Blatt als „Top-Spionin in der DDR“. Vor allem aber wurde sie mit dem Verschwinden des SED-Parteivermögens in Verbindung gebracht, wenngleich die Zeitung zugleich einräumte: „Es gibt derzeit keinerlei Beleg dafür, dass Kampa an möglichen kriminellen Machenschaften beteiligt war.“ Dennoch legte das Blatt eine Verwicklung Kampas in den schwer durchschaubaren Umgang mit den Vermögenswerten nahe. Kampa zog vor Gericht und verlangte eine Gegendarstellung. Sie bekam recht. Am 03.02.2014 druckte das Blatt ihre Antwort: „Mit dem Verbleib des SED-Vermögens nach 1989 hatte ich nichts zu schaffen.“

Springer hatte die Anordnung, Kampas Replik zu drucken, als Verletzung seiner Redefreiheit angesehen. Der Straßburger EGMR hingegen attestierte der deutschen Justiz, namentlich dem Berliner Kammergericht, sorgfältige Arbeit. Hier stehe der Schutz des Privatlebens gegen die Redefreiheit. Einen generellen Vorrang habe keine der beiden Positionen, beide Rechte verdienten vielmehr „den gleichen Respekt“. Im konkreten Fall habe das Kammergericht eine ausführliche und wohlabgewogene Prüfung des Artikels vorgenommen, die kein Anzeichen von Willkür trage. Auch sei die Antwort – gemessen an den durchaus detaillierten Ausführungen im Artikel – keineswegs unverhältnismäßig.

Umstritten war in dem Fall vor allem, ob Kampa irgendwie selbst schuld an dem Artikel war, weil sie – von der „Welt“ mit den Vorwürfen konfrontiert – nicht auf deren Fragen zu ihrer Beteiligung an Firmen mit angeblichem SED-Vermögen geantwortet hatte. Kampas Weigerung, dem Verlag Rede und Antwort zu stehen, stelle indes kein valides Argument dar. Das Gericht bestätigte, dass es zur journalistischen Ethik gehört, Betroffenen vor der Veröffentlichung eines Artikels die Gelegenheit zur Selbstverteidigung zu geben. Aber „die Tatsache, dass die Vorwürfe der Person im Voraus mitgeteilt wurden, gibt der Presse keine unbeschränkte Freiheit unbestätigte Vorwürfe zu veröffentlichen“. Auch das Recht auf Gegendarstellung werde dadurch nicht ausgehebelt. Der Gerichtshof stellt damit klar, dass die Nachfrage beim Betroffenen den Journalisten keinen Freibrief ausstellt, wenn die Antwort ausbleibt. Vorwürfe müssen trotzdem mit sorgfältiger Recherche abgesichert werden. Und wer als Betroffener schweigt, darf sich am Ende dennoch per Gegendarstellung äußern (Janisch, SZ 19.01.2023, 19).

EuGH

Eigentümerveröffentlichung zu juristischen Gesellschaften im Internet ist grundrechtswidrig

Der Europäische Gerichtshof (EuGH) Union sieht gemäß seinem Urteil vom 22.11.2022 einen schwerwiegenden und unverhältnismäßigen Eingriff in die Grundrechtecharta und erklärte die EU-Geldwäscherichtlinie zu Teilen für ungültig, soweit diese vorsieht, dass die Angaben zu wirtschaftlichen Eigentümern von Gesellschaften im Hoheitsgebiet der Gemeinschaft in allen Fällen für die Öffentlichkeit einsehbar sein müssen, um der Geldwäsche und der Finanzierung von Terrorismus entgegenzuwirken (Az. C-37/20, C-601/20).

Der mit dieser Maßnahme verbundene Eingriff in die durch die in Art. 7 und Art. 8 der Charta gewährleisteten Grundrechte auf Achtung des Privatlebens sowie auf den Schutz personenbezogener Daten sei weder auf das absolut Erforderliche beschränkt, noch stehe er in einem angemessenen Verhältnis zu dem verfolgten Ziel. Die Kläger hatten sich zunächst ohne Erfolg gegen ein im Jahr 2019 in Luxemburg erlassenes Gesetz zur Registrierung wirtschaftlicher Eigentümer gewandt, mit dem die Richtlinie umgesetzt wurde. Die gesammelten Informationen wurden – unter anderem über das Internet – der breiten Öffentlichkeit zugänglich gemacht. Die Kläger argumentierten mit der Gefahr von Erpressungen oder Entführungen und wollten den Zugang zu sensiblen Informationen einschränken lassen.

Nach Ansicht des EuGH ermöglichten es die verbreiteten Angaben einer potenziell unbegrenzten Zahl von Personen sich über die materielle und finanzielle Situation eines wirtschaftlichen Eigentümers Kenntnis zu verschaffen. Der Schutz gegen einen möglichen Missbrauch der Informationen sei nicht ausreichend und die entsprechende Bestimmung in der Richtlinie ungültig (EU-Geldwäscherichtlinie ist teilweise rechtswidrig, www.lto.de 22.11.2022).

EuGH

Google hat beim Recht auf Vergessen Ermessensspielraum

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 08.12.2022 entschieden, dass die Auslistung von Treffern einer Suchmaschine, die zu Falschangaben über die eigene Person führen,

keine Anhörung des Verursachers erfordert. Das Ersuchen sollte mit stichhaltigen Informationen belegt werden. „Fakes" müssen nicht schon gerichtlich festgestellt sein (C-460/20). Damit hat der EuGH in einem weiteren Verfahren zu komplizierten Fragen rund um das „Recht auf Vergessen" entschieden.

Geklagt hatten ein Geschäftsführer mehrerer Finanzdienstleistungsunternehmen und die Prokuristin eines dieser Unternehmen, weil Google der Auslistung kritischer Berichte eines in New York ansässigen Portals über die Firmen nicht stattgegeben hatte. Die fraglichen Berichte seien falsch und das Portal habe übrigens versucht sie zu erpressen, so die Klage. Die Kläger scheiterten in zwei Instanzen und wandten sich 2018 an den Bundesgerichtshof (BGH). Der legte 2020 dem EuGH die Frage vor, inwieweit die Kläger ihre Darstellung der Unwahrheit gerichtlich nachweisen müssen.

Die Große Kammer entschied: Wer Google zum Auslisten von seiner Meinung nach falschen Informationen nach Artikel 17 der DSGVO (Recht auf Vergessen) in Anspruch nimmt, muss nachweisen, dass es sich um Falschinformationen handelt. Es muss aber nicht gleich eine einstweilige Verfügung sein, um den Nachweis zu führen. Das wäre eine übermäßige Belastung des Einzelnen. Liegt ein gerichtlicher Titel in der Sache vor, dann muss die Suchmaschine auf jeden Fall auslisten. Es gebe keinen dem Persönlichkeitsrecht entgegenstehenden Anspruch der Öffentlichkeit auf freien Informationszugang; es gebe kein Recht auf Falsch-Information.

Im vorliegenden Fall konnten die Betroffenen gegenüber Google keinen Gerichtsbescheid vorweisen. In solchen Fällen ist der Betreiber der Suchmaschine nicht verpflichtet einem Auslistungsantrag stattzugeben, „wenn sich aus den von der betroffenen Person vorgelegten Nachweisen nicht offensichtlich ergibt, dass die in dem aufgelisteten Inhalt enthaltenen Informationen unrichtig sind". Es besteht ein Ermessensspielraum des Suchmaschinenbetreibers. Im Streitfall müsse den Betroffenen allerdings der Weg zum Gericht offenstehen, um die Ermessensentscheidung im Hause Google überprüfen zu lassen.

Der EuGH folgte in weiten Teilen den Schlussanträgen des Generalanwalts von April 2022. Anders aber beurteilten die Richter Googles Pflicht zur Mitwirkung bei der Wahrheitsfindung. Hatte Generalanwalt Giovanni Pitruzzella den Vorschlag unterbreitet, Google solle mit den zur Verfügung stehenden technischen Mitteln die erbrachten Nachweise überprüfen und, vor allem, „rasch ein Streitgespräch mit dem Herausgeber der Webseite, der die Information ursprünglich verbreitet hat, veranlassen", geht das Urteil nicht von einer Mitwirkungspflicht aus. Ein derartiger „procedural due data process" wäre für den Suchmaschinenbetreiber zu aufwändig und könne zur Neigung führen schneller auszulisten. Wie die Bewertung der von den Antragstellern beigebrachten Nachweise in der Praxis funktionieren wird, muss sich zeigen.

Vorgelegt hatte der BGH auch die Frage, ob Google Thumbnails mit Bildern der Kläger auslisten muss, die im Zusammenhang mit dem Artikel veröffentlicht worden waren. Der EuGH erkannte an, dass Vorschaubilder mit persönlichen Fotos „einen besonders starken Eingriff" ins Persönlichkeitsrecht darstellen. Der Suchmaschinenbetreiber müsse daher unabhängig vom Text prüfen, „ob die Anzeige der fraglichen Fotos erforderlich ist, um das Recht auf freie Information auszuüben". Besteht ein Auslistungsanspruch in Bezug auf den Artikel, müssen auf jeden Fall auch die Thumbnails gelöscht werden. Ist der Artikel über die Finanzdienstleistungsprodukte der Kläger ein wichtiger Beitrag zur Information der Öffentlichkeit, so kommt es darauf an, welchen Beitrag die Fotos zur Information der Öffentlichkeit darstellen. Das letzte Wort im konkreten Fall hat nun der BGH. (Ermert, Recht auf Vergessen: Keine Mitwirkungspflicht für Google bei Wahrheitsprüfung, www.heise.de 08.12.2022, Kurzlink: https://heise.de/-7370857).

EuGH

Anspruch auf konkrete Auskunft über Übermittlungsempfänger

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 12.01.2023 bekräftigt, dass gemäß dem Transparenzgrundsatz der Datenschutz-Grundverordnung (DSGVO) jeder Mensch das Recht hat zu erfahren, an wen seine personenbezogenen Informationen weitergegeben wurden (Az.: C-154/21). Dieser Anspruch gilt nicht absolut: Der für die Datenverarbeitung Verantwortliche kann sich darauf beschränken, nur die Kategorien von Empfängern mitzuteilen, wenn diese nicht einzeln identifizierbar sind. Ein Antrag darf auch nicht „offenkundig unbegründet oder exzessiv" sein. Der Oberste Gerichtshof Österreichs hatte den Fall dem EuGH vorgelegt.

Ein Bürger hatte die Österreichische Post unter Bezugnahme auf die DSGVO aufgefordert, ihm mitzuteilen, gegenüber welchen Empfängern sie seine personenbezogenen Daten offengelegt habe. Die Post teilte dem Anfragenden zunächst nur mit, sie verwende personenbezogene Daten – soweit rechtlich zulässig – im Rahmen ihrer Tätigkeit als Herausgeberin von Telefonbüchern und biete diese Daten Geschäftskunden für Marketingzwecke an. Der so Abgespeiste erhob daraufhin gegen die Aktiengesellschaft Klage vor den österreichischen Gerichten. Im Lauf des Verfahrens ließ sich die Post noch entlocken, persönliche Daten seien an Kunden weitergegeben worden, zu denen werbetreibende Unternehmen im Versandhandel und stationären Handel, IT-Unternehmen, Adressverlage und Vereine wie Spendenorganisationen, Nichtregierungsorganisationen oder politische Parteien gehört hätten.

Der EuGH entschied, dass der Verantwortliche verpflichtet ist, der betroffenen Person auf Anfrage die Identität der Empfänger mitzuteilen. Nur wenn es momentan oder künftig nicht möglich ist diese Adressaten individuell zu identifizieren, sei es legitim lediglich über die Kategorien der einschlägigen Empfänger Auskunft zu geben. Die Richter heben ferner hervor, dass das Auskunftsrecht erforderlich ist, um andere Betroffenenansprüche aus der DSGVO auszuüben, wie die Rechte auf Berichtigung, Löschung (auf „Vergessenwerden"), Einschränkung oder Widerspruch gegen die Verarbeitung oder Rechtsbehelf im Schadensfall. Das oberste österreichische Gericht muss nun prüfen, inwieweit die österreichische Post die-

sen Vorgaben genügte (Krempl, EuGH-Urteil: Bürger müssen wissen, wohin ihre Daten wandern, www.heise.de 12.01.2023, Kurzlink: https://heise.de/-7457616).

EuGH

Bei Einwilligungswiderruf sind sämtliche Verantwortliche zu informieren

Der Europäische Gerichtshof (EuGH) hat mit Urteil vom 27.10.2022 entschieden, dass für die Veröffentlichung personenbezogener Daten in einem öffentlichen Teilnehmerverzeichnis (Telefonverzeichnis) die vorherige Einwilligung des betreffenden Teilnehmers erforderlich ist (Az. C-129/21). Haben die Anbieter die Daten an andere Anbieter weitergeleitet, genügt es für einen Widerruf zur Erreichung der Datenlöschung, wenn sich der Betreffende an einen der „Verantwortlichen" wendet, der die anderen, auch Suchmaschinenbetreiber, zu informieren hat.

Der belgische TK-Anbieter Proximus bietet auch Teilnehmerverzeichnisse und Telefonauskunftsdienste an. Die Kontaktdaten (Name, Adresse und Telefonnummer) der Teilnehmer erhält er von anderen TK-Anbietern wie Telenet, es sei denn, der Teilnehmer hat den Wunsch geäußert nicht in die Verzeichnisse aufgenommen zu werden. Erhaltene Daten übermittelt Proximus außerdem an einen weiteren Anbieter von Teilnehmerverzeichnissen. Ein Telenet-Teilnehmer forderte Proximus auf seine Kontaktdaten in den Teilnehmerverzeichnissen nicht zu veröffentlichen. Proximus änderte den Status des Teilnehmers entsprechend. Allerdings erhielt Proximus von Telenet aktualisierte Daten des Teilnehmers, die nicht als vertraulich ausgewiesen waren und die erneut in ihren Teilnehmerverzeichnissen erschienen.

Nachdem der Teilnehmer seine Forderung erneuerte, antwortete Proximus, die Daten seien aus den Teilnehmerverzeichnissen gelöscht und Google kontaktiert worden, damit die maßgeblichen Links zur Proximus-Website entfernt würden. Das Unternehmen teilte außerdem mit, dass es seine Kontaktdaten an andere Anbieter von Teilnehmerverzeichnissen weitergeleitet habe, die dank der monatlichen Aktualisierungen über seine Forderung informiert worden seien. Der Teilnehmer legte zugleich Beschwerde bei der belgischen Datenschutzbehörde ein. Diese verpflichtete Proximus zur Abhilfe und verhängte gegen das Unternehmen wegen Verstößen gegen die DSGVO eine Geldbuße in Höhe von 20.000 Euro.

Proximus focht die Entscheidung beim Appellationshof Brüssel an und machte geltend, die Einwilligung des Teilnehmers sei für die Veröffentlichung seiner personenbezogenen Daten in Telefonverzeichnissen nicht erforderlich. Die Teilnehmer müssten selbst das „Opt-out" beantragen in den Verzeichnissen nicht aufgeführt zu werden. Die Datenschutzbehörde vertrat eine gegenteilige Auffassung. Der Appellationshof rief den EuGH an.

Der EuGH bestätigte, dass die Einwilligung eines ordnungsgemäß unterrichteten Teilnehmers für die Veröffentlichung seiner personenbezogenen Daten in einem öffentlichen Teilnehmerverzeichnis erforderlich sei. Diese Einwilligung erstrecke sich auf jede weitere Verarbeitung der Daten durch dritte Unternehmen, die auf dem Markt für öffentlich zugängliche Telefonauskunftsdienste und Teilnehmerverzeichnisse tätig seien, sofern diese Verarbeitung denselben Zweck verfolge. Die Einwilligung erfordere eine „in informierter Weise und unmissverständlich abgegebene" Willensbekundung in Form einer Erklärung oder einer sonstigen „eindeutigen bestätigenden Handlung", mit der die betroffene Person zu verstehen gebe, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden sei. Eine solche Einwilligung setze nicht unbedingt voraus, dass die betroffene Person zum Zeitpunkt ihrer Erteilung die Identität aller Anbieter von Verzeichnissen kenne, die ihre personenbezogenen Daten verarbeiten werden.

Der EuGH unterstreicht zudem, dass die Teilnehmer die Möglichkeit haben müssten die Löschung ihrer personenbezogenen Daten aus Teilnehmerverzeichnissen im Sinne der DSGVO zu erwirken. Ein Verantwortlicher wie Proximus müsse geeignete technische und organisatorische Maßnahmen ergreifen, um die anderen Anbieter von Teilnehmerverzeichnissen, denen er solche Daten geliefert hat, über den Widerruf der Einwilligung der betroffenen Person zu informieren. Er müsse zudem den Telefondienstanbieter, der ihm die Daten übermittelt hat, informieren. Wenn sich nämlich, wie im vorliegenden Fall, verschiedene Verantwortliche auf eine einheitliche Einwilligung der betroffenen Person stützten, genüge es, dass sich die betroffene Person, um ihre Einwilligung zu widerrufen, an irgendeinen der Verantwortlichen wende. Schließlich müsse ein Verantwortlicher wie Proximus nach der DSGVO angemessene Maßnahmen treffen, um Suchmaschinenanbieter über den bei ihm eingegangenen Antrag des Teilnehmers eines Telefondienstanbieters auf Löschung seiner personenbezogenen Daten zu informieren (Veröffentlichung von Kontaktdaten in Telefonverzeichnis nur mit Einwilligung, https://rsw.beck.de 27.10.2022).

BVerfG

Datenweitergabe von Verfassungsschutz an Polizei ist grundrechtswidrig

Gemäß einem Beschluss des Bundesverfassungsgerichts (BVerfG) vom 28.09.2022 verstößt die Weitergabe personenbezogener Daten durch die Verfassungsschutzbehörden an Strafverfolger in der aktuell praktizierten Form gegen das Grundrecht auf informationelle Selbstbestimmung, soweit die Gesetze zur Übermittlung personenbezogener Daten verpflichten, welche mit nachrichtendienstlichen Mitteln erhoben wurden (Az. 1 BvR 2354/13). Die diesbezüglichen Bestimmungen des Bundesverfassungsschutzgesetzes (BVerfSchG) verletzen das Trennungsprinzip und sind unverhältnismäßig. Strengere Bestimmungen für die Übermittlungen werden sich auch auf die Speisung der Rechtsextremismus-Datei (RED) auswirken.

§ 20 Abs. 1 S. 2 BVerfSchG regelt die Weitergabe von Personendaten durch

die Verfassungsschutzämter des Bundes und der Länder an Polizei und Strafverfolgung. Eine solche Weitergabe ist nach Ansicht der Richter nur auf Basis strenger Anforderungen überhaupt zulässig. Die Voraussetzungen, unter denen die Daten weitergegeben werden dürfen, sind nach Ansicht des Gerichts nicht klar geregelt. Die vom Beschwerdeführer, einem im Münchner Prozess wegen Beihilfe zum Mord verurteilten NSU-Helfer Carsten Schultze, angegriffene Regelung erlaubt das Durchreichen persönlicher Daten auf der Basis langer Listen von Straftatbeständen im Gerichtsverfahrensgesetz (GVG). Die dort aufgeführten Staatsschutzvergehen des GVG (Landesverrat, Bildung einer terroristischen Vereinigung usw.) werden als besonders schwerwiegend klassifiziert, wenn die Bundesanwaltschaft die Ermittlungen an sich zieht. Der Beschluss kritisiert die ungenügenden Differenzierungen bei der Gewichtung der Schwere der Straftat. Zwar seien Verweisungsketten üblich und nicht grundsätzlich zu beanstanden, doch müssten die Regelungen hinreichend bestimmt sein. Durch bloße Verweise auf die Listen werde gegen das Gebot der Verhältnismäßigkeit verstoßen, da die Straftaten in den §§ 120 und 74 GVG nicht unterschiedslos in die Kategorie „schwere Straftaten" fallen. Ein Beispiel ist der Verstoß gegen ein Vereinsverbot mit einer Höchststrafe von einem Jahr oder die Vorfeldregelung des § 89b Strafgesetzbuch (Aufnahme von Beziehungen zur Begehung einer schweren staatsgefährdenden Gewalttat).

Da Verfassungsschutzämtern sehr viel weiterreichende Mittel bei der Sammlung von Informationen zur Verfügung stehen, unterliegen die Übermittlungen gesteigerten Rechtfertigungsvoraussetzungen. Bei konkreter Gefahr können die Voraussetzungen durchaus erfüllt sein. Bei einer Neuregelung müsse der Gesetzgeber darauf achten „eine Übermittlung nicht zu weit im Vorfeld einer in ihren Konturen noch nicht absehbaren Gefahr" zu erlauben. Eine konkrete Gefahr müsse jeweils im Einzelfall festgestellt werden. In seinem Beschluss verweist das BVerfG erneut auf das Trennungsgebot zwischen Geheimdiensten und Strafverfolgern, das in den vergangenen Jahren mehr und mehr, etwa durch die gemeinsam genutzten Dateien wie die Antiterror-Datei und die Rechtsextremismus-Datei (RED), aufgeweicht wurde. Im Urteil zum Bayerischen Verfassungsschutzgesetz stand der Verstoß gegen dieses informationelle Trennungsgebot mit im Zentrum (DANA 2/2022, 127 f.). Weitere Verfassungsbeschwerden gegen Landesverfassungsschutzgesetze in Hessen und Hamburg sind anhängig. Für eine Novellierung der Übermittlungsbefugnisse im BVerfSchG hat das Bundesverfassungsgericht dem mit seinen Sicherheitsgesetzen wenig verfassungsfesten Gesetzgeber eine Frist bis Ende 2023 eingeräumt. Ungeklärt ist durch das BVerfG, was mit zu Unrecht übermittelten Personendaten passieren soll, die jetzt in der Rechtsextremismus-Datei gespeichert sind.

Beanstandet wurden vom BVerfG schließlich auch die in den Übermittlungsvorschriften geregelte Protokollierung, auch in Bezug auf die Nennung der in Anspruch genommenen Rechtsgrundlagen (Ermert, Verfassungsschutz: Karlsruhe schränkt Weitergabe von Daten an die Polizei ein, www.heise.de 03.11.2022, Kurzlink: https://heise.de/-7329062; BVerfG PM Nr. 85/2022 v. 03.11.2022, Erfolgreiche Verfassungsbeschwerde gegen die Übermittlung mit nachrichtendienstlichen Mitteln erhobener personenbezogener Daten; Janisch, Karlsruhe reguliert Datenfluss an Polizei, SZ 04.11.2022, 5).

EU-Gericht

WhatsApp-Bußgeld wegen Intransparenz bestätigt

Das EU-Gericht urteilte auf die Klage des Meta-Anbieters WhatsApp am 07.12.2022 erstmals über einen Antrag auf Nichtigerklärung einer verbindlichen EDSA-Entscheidung (Az.: T-709/21). Im August 2021 hatte die irische Datenschutzbehörde, die Data Protection Commission (DPC), auf Basis der europäischen Datenschutz-Grundverordnung (DSGVO) ein Bußgeld in Höhe von 225 Millionen Euro gegen WhatsApp verhängt (DANA 4/2021, 253). Die Aufsicht warf dem Messengerdienst mangelnde Information gegenüber den Betroffenen beim Teilen von Daten mit Facebook und weiteren Konzernunternehmen vor. WhatsApp bezeichnete die Sanktion als unverhältnismäßig und klagte dagegen nicht nur in Irland, sondern auch vor dem Gericht der EU. Die Luxemburger Richter wiesen diese Beschwerde als unzulässig zurück.

WhatsApp wandte sich an das EU-Gericht mit dem Antrag zum Annullieren einer vorgelagerten Entscheidung, weil der von der DPC zunächst vorgelegte Entwurf mit den Untersuchungsergebnissen und Strafempfehlungen in Kreisen der anderen nationalen Aufsichtsbehörden umstritten war. Die Vorlage ging daher an den Europäischen Datenschutzausschuss (EDSA), der Ende Juli 2021 einen für alle beteiligten Kontrolleure bindenden Beschluss fasste. Auf dieser Basis erließ die DPC wenig später ihre endgültige Verfügung. Ein solcher Rechtsakt ist demnach auf Basis des EU-Vertrags nicht direkt anfechtbar. Zudem sei WhatsApp von dem Beschluss des Datenschutzausschusses gar nicht unmittelbar betroffen. Die Gültigkeit der angefochtenen Entscheidung könne aber von dem nationalen Gericht geprüft werden, das mit einer Klage gegen den späteren endgültigen Beschluss befasst ist. In diesem Rahmen sei es auch möglich dem Europäischen Gerichtshof (EuGH) Fragen zur Vorabentscheidung vorzulegen.

Die angefochtene Entscheidung ändert gemäß dem Gerichtsentscheid an sich nichts an der Rechtsstellung von WhatsApp, da sie – anders als der endgültige Beschluss aus Irland – nicht unmittelbar gegen das Unternehmen vollstreckbar sei. Es handle sich nur um einen vorbereitenden Akt. Zudem habe die umstrittene EDSA-Entscheidung keine unabhängige Rechtswirkung gegenüber WhatsApp. Das EU-Gericht stärkt so auch insgesamt dem Datenschutzausschuss den Rücken. Der Messaging-Betreiber kann gegen das Urteil mit Bezug auf rein rechtliche Aspekte innerhalb von zwei Monaten und zehn Tagen Berufung vor dem EuGH einlegen (Krempl, Datenschutz: WhatsApp scheitert vor EU-Gericht mit Klage gegen Millionenstrafe, www.heise.de 12.12.2022, Kurzlink: https://heise.de/-7391950).

BGH

Erneut EuGH-Vorlage wegen Verbandsklagerecht

Der für Wettbewerbsrecht zuständige erste Zivilsenat des Bundesgerichtshofs (BGH) zieht mit seinem Beschluss vom 10.11.2022 ein zweites Mal vor den Europäischen Gerichtshof (EuGH) mit einer Detailfrage zum Klagerecht von Verbraucherschutzverbänden beim Datenschutz gegen große Tech-Plattformen (Az. I ZR 186/17). In dem Verfahren zwischen dem nach § 4 UKlaG eingetragenen Dachverband der Verbraucherzentralen, dem Verbraucherzentrale Bundesverband (vzbv), und der Internetplattform Facebook geht es darum, ob Verbraucherschützer auch ohne einen Auftrag konkret Betroffener vor Gericht ziehen dürfen. Auf eine erste BGH-Anfrage hin hatten die Luxemburger Richter entschieden, die Klagebefugnis des Verbandes stehe in Einklang mit der DSGVO (DANA 2/2022, 125).

In der Ende September 2022 fortgesetzten Verhandlung am BGH sah es so aus, als würden die obersten Zivilrichter Deutschlands dem folgen. Doch der erste Zivilsenat war von Anfang an der Meinung, dass Verbraucherschutzverbände nicht per se klagebefugt seien. Die anderslautende Entscheidung aus Luxemburg bezeichnete der Vorsitzende Richter Thomas Koch als „unerwartet". Der BGH legt deshalb nach und will wissen, ob in dem Fall aus Sicht des EuGH die Voraussetzung erfüllt ist, dass die Rechte einer betroffenen Person gemäß der DSGVO „infolge einer Verarbeitung" im Sinne von Art. 80 Abs. 2 DSGVO verletzt worden sind. Es sei fraglich, ob diese Voraussetzung erfüllt ist, wenn – wie im Streitfall – die sich aus Art. 12 Abs. 1 Satz 1, Art. 13 Abs. 1 Buchst. c und e DSGVO ergebenden Informationspflichten verletzt worden sind. Anwalt Peter Wassermann als Vertreter der Verbraucherschützer meinte bei der Verhandlung, eine Entscheidung in der Sache sei wichtig für eine „Fülle von Verfahren", die an Gerichten anhängig sind.

Der Leiter des Teams Rechtsdurchsetzung beim vzbv, Heiko Dünkel, bedauerte die durch die Entscheidung entstehende Hängepartie. Angesichts der massenhaften Datenschutzverstöße auf den großen Digitalplattformen sei es enttäuschend, dass sich dieses schon sehr lange laufende Grundsatzverfahren wieder verzögere: „Der vzbv wird sich nun mögliche Auswirkungen der heutigen Entscheidung auf weitere derzeit noch laufende Verfahren anschauen." Richter Koch räumte ebenfalls ein, es sei bedauerlich, dass sich das Verfahren nun erneut verzögere: „Aber es war unvermeidlich."

Der Facebook-Mutterkonzern Meta kommentierte den Beschluss nicht. Bei den konkret angemahnten Verstößen geht es darum, dass bei Facebook 2012 kostenlose Spiele von Drittanbietern präsentiert wurden, bei denen Nutzerinnen und Nutzer per Klick auf „Sofort-spielen" der Übermittlung verschiedener Daten an den Spielebetreiber zugestimmt hatten. Bei einem Spiel endeten die Hinweise mit dem Satz: „Diese Anwendung darf Statusmeldungen, Fotos und mehr in deinem Namen posten." Gerichte in Berlin gaben den Verbraucherschützern Recht. Der Anwalt von Facebook, Christian Rohnke, hatte bei der Verhandlung am BGH betont, Facebook habe diese Handhabe inzwischen geändert (BGH legt EuGH erneut eine Frage zur Klagebefugnis von Verbraucherschutzverbänden bei Datenschutzverstößen durch Facebook vor, BGH, PM Nr. 159/22 v. 10.11.2022; Datenschutz: Unklarheiten bei Klagerechten für Verbraucherschutzverbände, www.heise.de 10.11.2022, Kurzlink: https://heise.de/-7336293).

VG Ansbach

Private Fotobeweisübermittlung bei Verkehrsverstößen zulässig

Gemäß zwei Urteilen des Verwaltungsgerichts (VG) Ansbach vom 02.11.2022 darf, wer einen Falschparker anzeigen will, dessen Fahrzeug fotografieren und die Bilder der Polizei mailen ohne deswegen Probleme wegen des Datenschutzes zu bekommen (Az. AN 14 K 22.00468 u. AN 14 K 21.01431). Das Gericht gab damit zwei Männern Recht, die ihre Anzeigen von Parkverstößen auf Geh- und Radwegen, also von Ordnungswidrigkeiten, mit Fotos untermauert und deswegen vom Bayerischen Landesamt für Datenschutzaufsicht (BayLDA) eine Verwarnung samt einer Gebühr von 100 Euro bekommen hatten. Das beklagte BayLDA meinte, für die Anzeige einer Ordnungswidrigkeit würde die Angabe des Kfz-Kennzeichens samt Tatort und Tatzeit ausreichen. Die Klägerseite hielt dem entgegen, dass ohne fotografischen Beleg im Zweifel Aussage gegen Aussage stehe.

Einer der Kläger hatte zuvor mit der Polizei für ihn unangenehme Erfahrungen gemacht, nachdem er sich als Fahrradfahrer mehrfach über Falschparker auf Fahrrad- und Gehwegen aufgeregt hatte und in 17 Fällen mit Fotos der Autokennzeichen die Polizeiinspektionen Olympiapark und Moosach informiert hatte. Diese leitete keine Verfahren gegen die Falschparker ein, sondern meldete ihn beim BayLDA wegen der Verletzung des Persönlichkeitsrechts der Autofahrer. Der Leiter der Polizeiinspektion habe ihn zuvor, so die Darstellung des Klägers, persönlich angerufen: „Er hat sich gemeldet, um mich fertig zu machen." Die Anwohner würden durch die Falschparker nicht gestört, das sei kein Problem; er sei das Problem. Der Polizist habe damit gedroht ihn wegen Datenschutzverstoßes zu melden und ihn anzuzeigen, weil er in Zeiten der Pandemie das Haus verlassen habe.

Das VG verband die beiden Klageverfahren der Betroffenen wegen der identischen Fragestellungen zu einer gemeinsamen Verhandlung und stellte fest, dass es sich bei dem Vorgehen um eine rechtmäßige Datenverarbeitung gehandelt habe. Die Prozessbeteiligten stritten vor der 14. Kammer darum, ob die Anzeigenerstatter von den Parkverstößen persönlich betroffen sein müssen, um ein „berechtigtes Interesse" für die Datenübermittlung an die Polizei geltend machen zu können, und ob nicht die schriftliche oder telefonische Schilderung des Sachverhalts unter Angabe des Kfz-Kennzeichens ausreiche. Das BayLDA hatte darauf verwiesen, dass auf den Bildern oft auch andere Daten wie weitere Autos samt Kennzeichen oder Personen zu sehen seien. Die Kläger wiederum betonten, dass die Polizei sie aufgefordert habe die Parksituation zum Beweis mit Fotoaufnahmen möglichst genau zu dokumentieren.

Die Deutsche Umwelthilfe, die einen der beiden Kläger wegen der Bedeutung als Musterverfahren unterstützt,

begrüßte das Urteil durch ihren Bundesgeschäftsführer Jürgen Resch: „Falschparken ist kein Kavaliersdelikt, sondern gefährdet Menschen, die mit Fahrrad, Rollator, Rollstuhl oder Kinderwagen unterwegs sind. Die Behörden sollten nicht gegen zivilgesellschaftliches Engagement vorgehen, sondern konsequent Maßnahmen gegen zugeparkte Fuß- und Radwege, Falschparken vor abgesenkten Bordsteinen oder in Kreuzungsbereichen ergreifen. Und das nicht nur in Bayern, sondern bundesweit."

Das BayLDA erklärte, es werde die Verfahren zum Anlass nehmen Abstimmungsgespräche mit den zuständigen Ordnungsbehörden, insbesondere der Polizei aufzunehmen. Es sollten klare und einheitliche Informationen darüber erreicht werden, welche Angaben bei einer Anzeigeerstattung wegen Falschparkens verlangt werden und welcher Kommunikationsweg hierfür genutzt werden sollte. Nach Veröffentlichung der schriftlichen Urteilsgründe erklärte der Präsident des BayLDA, dass die Urteile nicht als „Freibrief für Falschparker-Fotografen" missverstanden werden dürften. In diesen Fällen sei die DSGVO mit den Datenminimierungs-, Lösch- und Auskunftspflichten umfassend anwendbar (Kehrhahn, DSGVO-Urteil: Bürger dürfen Falschparker für Anzeigen fotografieren, www.heise.de 03.11.2022, Kurzlink: https://heise.de/-7328875; DSGVO: Dürfen Bürger Falschparker für Anzeige fotografieren? www.heise.de 03.11.2022, Kurzlink: https://heise.de/-7328420; PE BayLDA 03.11.2022, BayLDA zu „Falschparker-Fotografen"-Entscheidung des VG Ansbach vom 03.11.2022; Wimmer, Falschparker dürfen fotografiert werden, SZ 04.11.2022, 24; BayLDA, PM v. 02.01.2023, Klageerfolg, aber kein Freibrief für „Falschparker-Fotografen").

VG Wiesbaden

Fluggastdatenabgleich ist illegal

Das Verwaltungsgericht (VG) Wiesbaden hat mit Urteilen vom 06.12.2022 in zwei Verfahren festgestellt, dass die vom Bundeskriminalamt (BKA) bislang praktizierte anlasslose und massenhafte Fluggastüberwachung mit dem EU-Recht und den darin verbrieften Grundrechten nicht vereinbar ist (Az.: 6 K 1199/22.WI u. 6 K 805/19.WI). In beiden Fällen ging es um die Verarbeitung sogenannter Passenger Name Records (PNR) nach dem Fluggastdatengesetz (FlugDaG), mit dem der Bundestag 2017 eine einschlägige EU-Richtlinie umzusetzen versuchte. Die Klagen hatten Malte Spitz, Generalsekretär der Gesellschaft für Freiheitsrechte (GFF), und der frühere EU-Beamte Emilio De Capitani 2019 eingereicht. Sie flogen jeweils auf innereuropäischen Strecken beziehungsweise von der EU aus in Drittstaaten und von dort zurück. In diesem Zusammenhang glich das BKA ihre Daten mit polizeilichen Datenbanken ab. Zu einem Treffer führte dies nicht.

Das VG gab den Feststellungsklagen statt mit der Begründung, dass es bei den innereuropäischen Flügen an einer grundrechtskonformen Rechtsgrundlage des BKA fehlte. Nach einem Grundsatzurteil des Europäischen Gerichtshofs (EuGH) dürften die Daten von Passagieren von Flügen innerhalb der EU nur verarbeitet werden, sofern es Anhaltspunkte für terroristische Bedrohungen auf bestimmten Flugrouten gebe (DANA 3/2022, 201 ff.). Eine solche Lage habe das BKA nicht nachweisen können. Die „Totalüberwachung sämtlicher Flüge", wie sie das FlugDaG vorsehe, sei daher unzulässig.

Auch bei den Flügen in einen Drittstaat liegt dem Gericht zufolge keine Rechtsgrundlage für die Datenverarbeitung durch das BKA vor. Die Bekämpfung gewöhnlicher Kriminalität rechtfertige es nach der EuGH-Rechtsprechung nicht die Informationen sämtlicher Flugpassagiere ohne konkreten Anhaltspunkt mit Ausschreibungs- und Fahndungsdatenbanken abzugleichen. Die Mitgliedstaaten haben laut der Ansage vielmehr die Aufgabe gesetzlich die schweren Straftaten zu benennen, wegen derer die Reisenden „einer so weitgehenden Datensammlung" ausgesetzt würden. Nur so könne sichergestellt werden, dass das System der Fluggastdatenspeicherung allein zur Bekämpfung schwerer Kriminalität eingerichtet und betrieben werde. Einen solchen Straftatenkatalog enthalte das FlugDaG aber nicht.

Mit der EU-Richtlinie können Flugpassagierdaten im Kampf gegen Terrorismus und Verbrechen grundsätzlich bis zu fünf Jahre lang gespeichert werden. Die PNR umfassen eine Vielzahl sensibler Informationen, die vom Geburtsdatum über die Namen der Begleitpersonen, eventuelle Vielfliegernummern oder die zum Kauf des Fluges verwendeten Zahlungsmittel bis hin zu einem Freitextfeld reichen. Die 6. Kammer des VG Wiesbaden hatte dem EuGH Fragen zur Vereinbarkeit der Richtlinie mit höherrangigem EU-Recht wie der Grundrechtecharta gestellt. Diese haben die Luxemburger Richter zwar noch nicht direkt beantwortet. Dafür erklärten sie im Juni 2022 auf eine ähnliche Vorlage des belgischen Verfassungsgerichtshofs hin, dass die Richtlinie prinzipiell Bestand habe. Entsprechende nationale Befugnisse müssten auf das „absolut Notwendige" beschränkt werden (DANA 3/2022, 201 f.). Damit zeichnete sich bereits ab, dass das BKA seine Rasterfahndung im Himmel deutlich zurückfahren muss.

Spitz freute sich über einen „Erfolg gegen Massenüberwachung". Der lange Atem habe sich gelohnt. Weitere Klagen, die die GFF koordiniert, sind bei anderen deutschen Gerichten gegen das BKA und Fluglinien wie die Lufthansa noch anhängig. Die Bundesregierung hatte das Vorgehen 2020 als verhältnismäßig verteidigt. Die Fluggastdatenzentrale im BKA verarbeitete im gleichen Jahr rund 105 Millionen Passagierdatensätze. Die Trefferquote für potenzielle Gefährder lag 2019 bei 0,082 Promille.

Das BKA kann beim Hessischen Verwaltungsgerichtshof Berufung einlegen. Auch die Option zur Sprungrevision beim Bundesverwaltungsgericht ließ die Kammer offen. Rechtsmittel müsste die Polizeibehörde binnen eines Monats einlegen. Die EU-Länder überlegen derweil, ob sie dauerhaft eine „reale und aktuelle oder vorhersehbare terroristische Bedrohung" deklarieren könnten (VG Wiesbaden, PE Nr. 07/2022, Verarbeitung von Fluggastdaten rechtswidrig; Krempl, Fluggastdaten: Verwaltungsgericht untersagt BKA Himmels-Rasterfahndung, www.heise.de 28.12.2022. Kurzlink: https://heise.de/-7443833).

LG Frankfurt am Main

Auch sinngleiche Ehrverletzungen sind umfassend in Social Media zu löschen

Das Landgericht (LG) Frankfurt am Main hat auf Antrag des Antisemitismusbeauftragten des Landes Baden-Württemberg, Michael Blume, im Eilverfahren am 14.12.2022 entschieden, dass ehrverletzende und falsche Tweets von Twitter gelöscht werden müssen, wenn Betroffene das verlangen (Az. 2-03 O 325/22). Auch „kerngleiche", also sinngemäße, leicht umformulierte Kommentare mit identischem Äußerungskern muss Twitter entfernen, sobald es von der konkreten Persönlichkeitsrechtsverletzung Kenntnis erlangt. In Bezug auf Facebook hat das so bereits der Europäische Gerichtshof (EuGH) im Jahr 2019 entschieden (DANA 4/2019, 235 f.).

Auf Twitter behaupteten Nutzer wahrheitswidrig, Blume habe „eine Nähe zur Pädophilie" und er habe „einen Seitensprung gemacht". Er sei in „antisemitische Skandale" verstrickt und „Teil eines antisemitischen Packs". Mehrfach meldete Blume, der durch die gemeinnützige Organisation HateAid im Verfahren unterstützt wurde, im durch das Netzwerkdurchsetzungsgesetz (NetzDG) eingeführten Verfahren die Kommentare. Nach dem NetzDG hätte Twitter ihm demnach eine Beschwerdemöglichkeit einräumen müssen. Außerdem hätte die Plattform ihn auf die Option hinweisen müssen Strafanzeige gegen den Verfasser zu erstatten. Twitter hatte zunächst nahezu alle Kommentare online stehen gelassen. Erst mehr als eine Woche nach der Meldung waren sie verschwunden. Dies geschah aber nicht, weil Twitter sie dauerhaft entfernte, sondern, so HateAid, weil der für die Verleumdungen hauptverantwortliche Account gesperrt wurde.

Blume wollte aber, dass Twitter die Kommentare löscht. Das LG stellte fest, dass diese ehrenrührigen Behauptungen unwahr sind. Die Bezeichnung „Antisemit" sei zwar eine Meinungsäußerung. Sie sei aber in diesem Kontext rechtswidrig, denn sie trage nicht zur öffentlichen Meinungsbildung bei. Vielmehr ziele sie erkennbar darauf ab Stimmung gegen den Antisemitismusbeauftragten zu machen. Twitter hätte nach der Aufforderung des Antisemitismusbeauftragten die Kommentare zu löschen, ihre Verbreitung unverzüglich unterlassen und einstellen müssen: „Das Unterlassungsgebot greift nicht nur dann, wenn eine Äußerung wortgleich wiederholt wird, sondern auch, wenn die darin enthaltenen Mitteilungen sinngemäß erneut veröffentlicht werden."

Allerdings seien die Äußerungen nicht in jeglichem Kontext zu untersagen. Betroffen seien nur solche Kommentare, die als gleichwertig anzusehen seien. Der Äußerungskern müsse identisch sein. Twitter habe auch keine allgemeine Monitoring-Pflicht im Hinblick auf seine rund 237 Millionen Nutzenden. Prüfen müsse die Plattform nur konkret beanstandete Persönlichkeitsrechtsverletzungen.

Als zulässig erachtete die Kammer die Äußerung eines Nutzers, wonach der Antisemitismusbeauftragte in die jährlich vom Wiesenthal-Zentrum in Los Angeles veröffentlichte Liste der größten Antisemiten weltweit aufgenommen worden ist. Das Center, das mit dem echten Simon Wiesenthal nichts gemeinsam hat außer den Namen und deshalb unseriös daherkommt, hat Blume tatsächlich so eingestuft. Es gehe nicht um die Frage, ob die Aufnahme gerechtfertigt sei. Es ginge um die Information über die Aufnahme in der Liste. Darüber dürfe grundsätzlich informiert werden. Dagegen müsse sich der Antisemitismusbeauftragte im öffentlichen Meinungskampf zur Wehr setzen.

HateAid begrüßte das Urteil grundsätzlich, übte jedoch auch Kritik: „Eine Klage darf nicht die einzige Möglichkeit sein, um sein Recht auf Social-Media-Plattformen durchsetzen zu können. Diese systemischen Defizite in der Content-Moderation auf Twitter beobachten wir schon länger – meist lassen sie Betroffene hilflos zurück." Blume wurde von Rechtsanwalt Chan-jo Jun von Jun Rechtsanwälte vertreten: „In einer idealen Welt bemühen sich Unternehmen die für sie geltenden Gesetze so gut wie möglich zu befolgen. Twitter stellt sich inzwischen dazu im Widerspruch. Mit der Entscheidung wird es künftigen Opfern viel leichter sein ihre Rechte durchzusetzen" (Twitter muss ehrverletzende Tweets löschen, www.lto.de 14.12.2022; Steinke, Und es gibt doch eine Pflicht, SZ 15.12.2022, 4).

LG München I

IAB-Cookie-Einwilligungsmanagement verstößt gegen TTDSG

Das Landgericht (LG) München I hat mit Urteil vom 29.11.2022 in einem Verfahren gegen BurdaForward, eine Tochter von Hubert Burda Media, entschieden, dass der Cookie-Banner auf Focus Online gegen das Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) verstößt (Az. 33 O 14776/19). Die Richter gaben den Verbraucherschützern nicht in allen Punkten recht. Die Entscheidung ist nicht rechtskräftig. Sie erging als erste in einer Reihe von Verfahren des Verbraucherzentrale Bundesverbands (vzbv) gegen die heute üblichen Cookie-Banner. Mit den Verfahren betritt der Dachverband der Verbraucherzentralen in vieler Hinsicht juristisches Neuland. Für dessen administrative Bewertung sind die Datenschutzbeauftragten der Länder zuständig. Mehrere dieser Behörden hatten 2020 eine Prüfung von Verlags-Websites initiiert. Öffentlich bekannte Sanktionen oder andere spürbare Auswirkungen hatte dies jedoch bisher nicht.

Die Verbraucherschützer reichten Klage gegen insgesamt fünf große deutsche Verlage ein. Zunächst war die Klagebefugnis des vzbv wegen Verstößen gegen die Datenschutz-Grundverordnung (DSGVO) von vielen Unternehmen bestritten worden. Nach einer Vorlage durch den Bundesgerichtshof (BGH) beim Europäischen Gerichtshof (EuGH) war diese Frage grundsätzlich geklärt. Es bedarf keiner individualisierten Beschwerden (DANA 2/2022, 125). Mit Beschluss vom 10.11.2022 richtete der BGH überraschend eine zweite Anfrage an den EuGH, um zu klären, ob der vzbv tätig werden darf, obwohl die DSGVO voraussetzt, dass ein Verstoß „infolge einer Verarbeitung" vorliegen müsse (s.o. S. 64).

Das LG München wollte mit seiner Entscheidung nicht auf diese Klärung

warten. Demnach darf der Verlag keine „domainübergreifende Aufzeichnung des Nutzerverhaltens zu Analyse- und Marketingzwecke“ vornehmen, wenn die Zustimmung dazu nicht deutlich anders gestaltet wird. Das Gericht sieht die bisherige Praxis auf Focus Online nicht als geeignet dafür eine „informierte und freiwillige Einwilligung“ der Nutzer zu erlangen. Alleine die Screenshots der zum Klagezeitpunkt 2019 auf Focus Online eingesetzten Cookie-Banner umfassen in der Gerichts-Entscheidung 141 Seiten, was offensichtlich zu viel Information ist, um vom durchschnittlichen Verbraucher hinreichend gewürdigt zu werden. Selbst wer scheinbar die Einwilligung auf der ersten Ebene verweigerte, musste noch viele Cookies hinnehmen, bei denen sich BurdaForward auf ein „berechtigtes Interesse“ berief Nutzerdaten zu verarbeiten und weiterzugeben. Neben dem Einsatz von Cookies bemängelten die Verbraucherschützer auch andere Formen des Trackings: das Browser-Fingerprinting, die Einbindung von Skripten, iFrames und die Erfassung von IP-Adressen.

Der beklagte Verlag verwies darauf, dass die Gestaltung des Cookie-Banners auf Focus Online marktüblich sei und Leser gar nicht alle Seiten des Cookie-Banners zur Kenntnis nehmen müssten. Die Nutzer hätten die „Zweistufigkeit“ solcher Dialoge mittlerweile gelernt. Auch sehe das Gesetz nicht vor, dass die Nutzer auf der ersten Ebene eines Cookie-Banners mit einem Klick alle Datenverarbeitungen ablehnen können sollten.

Bei seinem Cookie-Banner stützt sich der Verlag wesentlich auf das Transparency and Consent Framework (TCF) der Werbeorganisation IAB Europe, mit dessen Hilfe die Zustimmung von Nutzern per einzelnem Klick an oft über hundert Drittparteien weitergegeben werden kann. Die zuständige belgische Datenschutzbehörde hatte das Verfahren bereits im Februar für unzulässig erklärt (DANA 2/2022, 114 f.). Gegen die Aufsichtsentscheidung hat IAB Europe Rechtsmittel eingelegt. Der Burda-Verlag stellte sich auf den Standpunkt, dass der TCF und der übermittelte „Consent String“ den gesetzlichen Vorgaben genüge und keine Informationen darüber enthalte, welche Apps oder Websites ein Nutzer besucht habe. Alles in allem biete die Übermittlung des Einverständnisses alleine „keine sehr intimen Einsichten“.

Das LG München I folgte dieser Argumentation nicht. Der TC-String sei eindeutig eine personenbezogene Information, zu deren Übermittlung gerade die individuelle Zustimmung nötig sei. Da mit dem TC String auch notwendigerweise eine IP-Adresse übertragen werde, sei ein Abgleich mit anderen Daten und damit eine Identifizierung möglich. Ebenso lehnte das Gericht die Argumentation ab, dass der Website-Betreiber selbst nicht verantwortlich sei, wenn Dritte Cookies abspeichern. Ob der Verlag Cookie-Banner auf Basis des TCF einsetze, sei seine eigene Entscheidung.

Das LG teilte auch nicht das Argument, die Nutzer würden für die Verarbeitung ein gültiges Einverständnis erteilen: „Als freiwillig kann die Einwilligung nur dann betrachtet werden, wenn die betroffene Person tatsächlich eine Wahlmöglichkeit hat, das heißt auch ohne Nachteile auf die Erteilung der Einwilligung verzichten kann.“ Der Aufwand die Einwilligung zu verweigern, sei angesichts der im Internet üblichen Schnelligkeit zu hoch.

Ein berechtigtes Interesse könne nicht als Rechtfertigung für die Datenverarbeitung herhalten. Zwar beklagen Verlage, dass ohne solche Datenverarbeitung die Refinanzierung journalistischer Inhalte kaum möglich ist: „Es handelt sich dabei lediglich um subjektive Interessen der Beklagten.“ Weitergehende Anträge der Verbraucherschützer lehnten sie aber ab, da sich die Klage nur auf das deutsche TTDSG und nicht auf die DSGVO direkt bezog.

Rosemarie Rodden, Referentin beim vzbv, zeigte sich mit dem Urteil zufrieden: „Sehr erfreulich ist, dass sich das Gericht unserer Ansicht angeschlossen und festgestellt hat, dass die mit dem Cookie-Banner eingeholte Einwilligung nicht auf einer freiwilligen Entscheidung der Nutzer beruht. Das Gericht hat bestätigt, dass Cookies, die der domainübergreifenden Nachverfolgung zu Analyse- und Marketingzwecken dienen, für den Betrieb eines Nachrichtenportals nicht technisch unbedingt erforderlich sind.“ Der Verband wolle nun prüfen, inwieweit man die Klagen in den parallel laufenden Verfahren weiter anpassen kann.

Auf Seiten des Verlags sieht man dies naturgemäß anders. Burda beharrt darauf, dass das Einwilligungsmanagement bei Focus Online „sowohl den geltenden Gesetzen als auch zu jeder Zeit den gängigen Marktstandards“ entspricht. Das Landgericht habe sich mit dem Urteil zu einigen „höchstrichterlich ungeklärten und kontrovers diskutierten Rechtsfragen“ positioniert, weshalb der Verlag plant, Rechtsmittel gegen das Urteil einzulegen (Kleinz, Verbraucherschützer klagen erfolgreich gegen Cookie-Banner, www.heise.de 19.12.2022, Kurzlink: https://heise.de/-7408270; Datenschutz-Streit wird erneut Fall für EuGH, www.lto.de 10.11.2022).

SG München

TI-Anschlusspflicht ist rechtmäßig

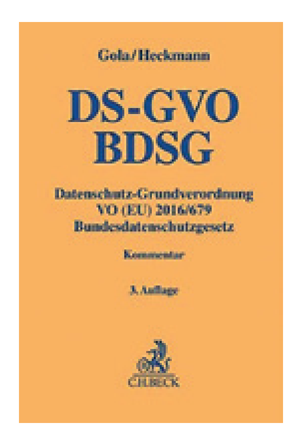
Das Sozialgericht (SG) München hat mit Urteil vom 26.01.2023 die Klage eines Arztes gegen Honorarkürzungen im Zusammenhang mit der verpflichtenden Anbindung an die Telematikinfrastruktur (TI) – dem deutschen Gesundheitsnetz – abgewiesen. Demgemäß ist es nicht ersichtlich, dass die einschlägigen Vorschriften im Sozialgesetzbuch (SGB) V gegen die Datenschutz-Grundverordnung verstoßen. Nach einer etwa fünfstündigen Verhandlung hatte das Gericht gut eine Stunde hinter verschlossenen Türen beraten. Der Augenarzt Gernot Petzold aus Kulmbach hatte sich mit seiner Klage gegen den Abzug von einem bis zu 2,5% der Kassen-Vergütung gewendet. Seit einigen Jahren sind Ärzte und Psychotherapeuten verpflichtet sich an die TI anzuschließen, über die Patientendaten ausgetauscht werden. Petzold sieht die ärztliche Schweigepflicht und die Sicherheit der Patientendaten gefährdet und verweigert sich dem Anschluss: „Es ist für mich nicht kontrollierbar, wer die Daten nutzen kann. Dadurch ist das Persönlichkeitsrecht der Patienten verletzt. Ich sehe die gesamte ärztliche Behandlung in Gefahr, wenn die Menschen nicht mehr vertrauensvoll mit dem Arzt reden können. Solche Daten müssen beim Arzt bleiben.“ Verschiedene Institutionen und Firmen, darunter Pharmafirmen, IT-Unternehmen und Hersteller medizi-

nischer Geräte, hätten Interesse an den Daten. Zudem gebe es immer wieder Hackerangriffe. „Einen Anschluss meines Praxisservers ans Internet – das will ich nicht. Ich habe eine voll digitalisierte Praxis, aber das System ist in sich geschlossen."

Petzold ist Vorstandsmitglied des Bayerischen Facharztverbandes (BFAV). Er kündigte an Berufung einzulegen und notfalls bis zum Bundesverfassungsgericht oder zum Europäischen Gerichtshof zu ziehen. Beklagt war die Kassenärztliche Vereinigung Bayern (KVB). Nach deren Angaben sind rund 1.600 von rund 17.600 Praxen in Bayern nicht an die TI angeschlossen und müssen gemäß Gesetz jedes Quartal einen Honorarabzug hinnehmen. Das SG München hatte schon im November 2022 eine ähnlich lautende Klage eines Zahnarztes abgewiesen. In Stuttgart hatte ein Arzt ebenfalls ohne erstinstanzlichen Erfolg geklagt. Weitere Klagen sind anhängig. Eine Sprecherin des SG meinte, die Sache müsse letztlich wohl höchstrichterlich vom Bundessozialgericht entschieden werden. Es gehe um grundsätzliche Fragen, insbesondere, ob die gesetzlich festgelegte Verpflichtung mit höherrangigem Recht wie dem Grundgesetz und der Datenschutz-Grundverordnung der EU vereinbar sei.

Die KVB erklärte nach der Entscheidung: „Auch nach dem heutigen Beschluss des Sozialgerichts bleiben wir dabei: Repressionen und Sanktionen wie die Honorarkürzungen bei Nichtanbindung an die Telematikinfrastruktur sind der falsche Weg, um innerhalb der Ärzteschaft Akzeptanz für die Digitalisierung des Gesundheitswesens zu schaffen." Die Politik sei gefordert gemeinsam mit Ärztinnen und Ärzten eine zukunftsfähige Strategie zu entwickeln, wie die Informationstechnologie nutzbringend für Praxen und Patienten eingesetzt werden könne (Sorge um Schutz von Patientendaten: Gericht weist Klage eines Arztes ab, www.heise.de 27.01.2023, Kurzlink: https://heise.de/-7472301; Sorge um Schutz von Patientendaten: Gericht weist Klage ab, www.sueddeutsche.de 26.01.2023).

Buchbesprechungen



Gola, Peter/Heckmann, Dirk
Datenschutz-Grundverordnung Bundesdatenschutzgesetz
Kommentar, Verlag C.H.Beck München, 3. Aufl. 2022
ISBN 978-3-406-78266-4, 1864 S., 99,00 €

(tw) Niemand kann behaupten, dass es zur DSGVO nicht genügend Kommentierungen gäbe. Was sich schon nach der Verabschiedung der DSGVO abzeichnete, findet auch nach vier Jahren Anwendbarkeit kein Ende – inzwischen angereichert durch Kommentierungen zum BDSG. Der „Gola" hat ein lange Geschichte: Begründet wurde die Kommentierung des uralten BDSG von Ordemann/Schomerus. 1992 erschien dann die 5. Auflage erstmals mit Peter Gola und Rudolf Schomerus. Es folgten viele weitere Auflagen, die immer dicker und auch schwerer zu lesen wurden. Das BDSG wurde geändert, zuletzt völlig, nachdem es an die Vorgaben der DSGVO angepasst werden musste. So erschien 2019 die 13. Auflage, diesmal mit herausgegeben von Dirk Heckmann (DANA 2/2019, 113). Das BDSG wurde zu einer teilweise die DSGVO nur noch ergänzenden Rumpfregelung. Die DSGVO wurde derweil auch von Gola herausgegeben kommentiert, 2018 schon in zweiter Auflage (DANA 3/2018, 160). Es war und ist naheliegend, dass nun die beiden Kommentierungen zusammengeführt zwischen zwei Buchdeckeln erscheinen. Dies erspart Doppelkommentierungen sowie ein Hin und Her. Auch Konkurrenzprodukte liefern gemeinsame Kommentierungen von DSGVO und BDSG.

Die Zahl der Kommentierer:innen hat weiter zugenommen. Inzwischen zeichnen 30 Personen für den Inhalt verantwortlich – viele seit Jahren, einige neu dabei.

Nicht nur die Zahl der Autor:innen zeigt, dass zumindest für den Juristenstand der Datenschutz etabliert ist. Quellen finden sich bei Gerichten, in Fachartikeln und in einer Vielzahl von Veröffentlichungen der Aufsichtsbehörden sowie derer Zusammenschlüsse (Europäischer Datenschutzausschuss, DSB-Konferenz). Hier noch den Überblick zu wahren und à jour zu bleiben ist nicht einfach. Hier helfen gute Kommentierungen – zu denen der aktuelle Gola/Heckmann gehört. Kommentiert werden nicht nur die §§ 1 bis 44, sondern auch die §§ 45 bis 86 BDSG zu Polizei und Justiz. Dies kann aber nur rudimentär bleiben, zumal die Hauptregelungen zu Polizei und Justiz im spezifischen Recht zu finden sind. Das neue TTDSG ist berücksichtigt, wird aber nicht speziell kommentiert. Zwar differiert die Qualität von Autorin zu Autor, doch durchgängig ist sie gut, aktuell und verlässlich. Anders als die Großkommentare sind die Texte noch übersichtlich, so dass die Nutzung nicht gleich zu einer wissenschaftlichen Arbeit werden muss. Dennoch ist das Buch auch zum vertieften Einstieg geeignet. Die Verweise sind vielfältig und – soweit das bei den über 1800 Seiten beurteilt werden kann – weitgehend vollständig.

Es handelt sich um einen Praxiskommentar an ein wenig differenziertes Publikum. Dies hat zur Folge, dass nicht

von allen Autor:innen eine bürgerrechtliche Linie verfolgt wird. Erfreulich ist aber, dass Autoren, die ehedem eine weniger betroffenenfreundliche Linie verfolgt haben, sich aktuellen positiven Entwicklungen bei der Aufsicht oder bei Gerichten anschließen, oder diese zumindest darstellen. D.h. referiert wird der „Mainstream", eher selten eine kritische Sichtweise, die ja angesichts der Schlampigkeit des deutschen Gesetzgebers an vielen Stellen angebracht und notwendig ist. Dieses Defizit weisen aber fast alle Kommentare mit diesem Gegenstand auf, vielleicht abgesehen vom Großkommentar Simitis/Hornung/Spiecker (DANA 1/2019, 34) sowie dem sich auf Beschäftigtendatenschutz fokussierenden Däubler/Wedde/Weichert/Sommer (DANA 3/2018, 161).

Erfreulich ist auch der Preis, der das Werk erschwinglich macht. Für Anwendende im allgemeinen Datenschutz also zu empfehlen, nicht nur als Einstieg, regelmäßig, aber eben nicht immer, ausreichend für die abschließende Beantwortung von praktischen Fragen.



Rost, Martin
Das Standard-Datenschutzmodell (SDM)
Einführung, Hintergründe und Kontexte zum Erreichen der Gewährleistungsziele
Springer Vieweg Wiesbaden, 2022
ISBN 978-3-658-38879-9, 223 S., 59,95 €, ISBN 978-3-658-38880-5 (eBook), 46,99 €

(tw) Während die Literaturlage in Sachen Datenschutzrecht üppig ist, kann das über das Angebot zum Thema technischer Datenschutz so nicht gesagt werden. Zwar gibt es auch hierzu haufenweise Aufsätze – insbesondere zu Einzelthemen – und auch spezifische Buchveröffentlichungen, doch eine konsistente allgemeine, auch für den engagierten Laien verständliche Darstellung gab es bisher noch nicht. Bisher. Dieses Defizit wird durch das Werk von Rost behoben. Es wendet sich aber vor allem an Insider. Schon mit dem Titel „Standard-Datenschutzmodell", kurz SDM, können Nicht-Datenschützer zunächst nichts anfangen. Dass es sich hierbei um ein im Rahmen der Kooperation der Datenschutzaufsichtsbehörden entwickeltes Konzept zur technischen Umsetzung und Kontrolle technisch-organisatorischer Datenschutz-Maßnahmen (TOM) handelt, ist außerhalb der Szene nicht bekannt. Doch auch für Insider ist der Begriff bisher wenig greifbar, ja, er ist fast mystisch – als sei das SDM die Allzweckwaffe, mit der alle Fragen zum technischen Datenschutz beantwortet werden könnten, wenn man sich nur tief genug damit befassen würde, wovon man aber eher zurückschreckt.

Bei der Lektüre des Buchs werden wir eines Besseren belehrt: Das SDM ist nichts Geheimnisvolles, Schwieriges, auch nicht abschließend Vollständiges. Es handelt sich um eine entwicklungsfähige Methode, mit der technischer Datenschutz in die Praxis umgesetzt wird. Und das ist kein Hexenwerk, wenn auch nicht ganz einfach. Den Zugang hierzu liefert Rost mit seinem Buch.

Der Autor ist hier prädestiniert – durch seine vielen Jahre Aufsichtserfahrung beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein (ULD), vor allem aber als derjenige, der die ursprünglich auf Andreas Pfitzmann zurückgehende Idee der Systematisierung von Schutzzielen über Jahre hinweg bis heute begleitet und maßgeblich vorangetrieben und inzwischen mit dem SDM zu einer erfolgreichen und anerkannten Methode gereift hat. Er erweist sich dabei nicht nur als fachlich kompetent, sondern auch pädagogisch, wie er mit einer einfachen und klaren Sprache didaktisch klug das Anliegen des SDM und den Umgang mit dem SDM vermittelt, durch Wiederholungen, das Eingehen auf sich aufdrängende Bedenken und durch Aufgaben zwecks Reflektion durch den Leser. Dies tut er nicht belehrend, aber mit schonungsloser Klarheit – auch gegenüber den vielen Dilettanten, die sich auf dem Feld des technischen Datenschutzes tummeln und äußern. Er erklärt, setzt sich mit anderen Positionen auseinander und beschränkt sich nicht – was weit verbreitet ist – auf das Abarbeiten von Checklisten.

Statt also gleich mit Maßnahmen zu beginnen, verfolgt Rost einen ganzheitlichen Ansatz, indem er zunächst die zentrale Funktion des informationellen Grundrechtsschutzes definiert, nämlich die Machtasymmetrie zwischen datenverarbeitender Organisation und Betroffenen zu kompensieren und deren Datenverarbeitung fair zu gestalten, und indem er dann auch die rechtlichen Instrumente der DSGVO erläutert.

Erhellend ist das beschriebene systematische Vorgehen. So werden zunächst die Gewährleistungsziele Datenminimierung (als Konkretisierung der Nichtverkettung) – Verfügbarkeit – Integrität – Vertraulichkeit – Nichtverkettung – Transparenz – Intervenierbarkeit aus den Zielen des Art. 5 DSGVO abgeleitet und in ein Verhältnis gesetzt. Keines der Ziele, die zueinander in Konflikt stehen können, darf absolut gesetzt werden. Es bedarf einer Zieloptimierung im Anwendungsfall. Hierbei ist nach Verarbeitungsschritten zu differenzieren: von der Erhebung über die Speicherung und die Nutzung bis zur Löschung. Jedes der Ziele wird mit Maßnahmen in Verbindung gebracht – den berühmten TOM – und im Hinblick auf die Risiken zugeordnet. Dabei differenziert Rost, der DSGVO folgend, zwei Risikoklassen: normales und hohes Risiko. Er orientiert sich aber hinsichtlich der nötigen Maßnahmen daran, dass auch schon ohne weitere Folgen mit der reinen Verarbeitung personenbezogener Daten ein Eingriff erfolgt.

Um keine Risiken zu übersehen und eine umfassende technische Gewährleistung des Datenschutzes sicherzustellen, wird der SDM-Würfel vorgestellt, bei dem auf sämtlichen Verarbeitungsebenen (Fachlogik, konkrete Sachbearbeitung, Infrastruktur) und allen Verarbeitungsphasen sämtliche Gewährleistungsziele durchdekliniert werden. Die TOM werden beschrieben, wobei der Schwerpunkt auf die datenschutzspezifischen TOM gesetzt werden, ohne aber die klassischen IT-Sicherheits-TOM zu vernachlässigen. Es sind auch genau diese (z.B. Protokollierung, Mandan-

tentrennung, Rollenkonzept), die im SDM von den Aufsichtsbehörden bisher besonders in den Fokus genommen werden. Die regelmäßige Anwendung des Instruments des SDM ist im Rahmen eines Datenschutzmanagements sinnvoll.

Der Autor beschreibt, aufbauend auf der Geschichte der SDM-Methode, deren Verhältnis zu den Schutzzielen der Informationssicherheit sowie zu verwandten Instrumenten. Das vorrangige Schutzobjekt der IT-Sicherheit ist die Organisation. Der Datenschutz hat dagegen den Betroffenen im Blick. Die anzuwendenden Maßnahmen ergänzen sich aber hervorragend. Rost stellt dar, wie das SDM bei der Erstellung von Verarbeitungsverzeichnissen, v.a. aber bei der Datenschutz-Folgenabschätzung und bei Datenschutz-Zertifizierungen nützlich eingesetzt werden kann.

Erfreulich ist der Stil des Buchs: Es ist meinungsstark parteiisch und zugleich faktenbasiert und mit vielen Beispielen versehen. Damit ist der Autor in der Lage seine eigene Begeisterung auf den Leser zu übertragen. Jedes Kapitel ist mit weiterführenden Literaturhinweisen versehen; ein Stichwortverzeichnis ermöglicht die Nutzung sowohl als Lern-, als auch als Umsetzungs- und Nachschlagewerk. So ist das Buch von Rost zugleich Einführung, Vertiefung und Gebrauchsanweisung für jede und jeden, die und der mit operativem Datenschutz zu tun hat.



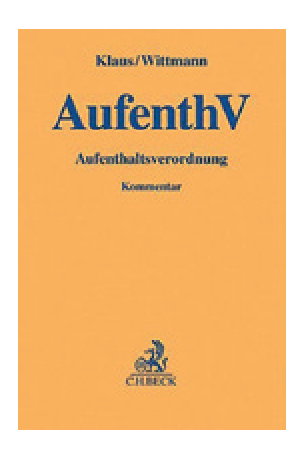
Däubler, Wolfgang
Digitalisierung und Arbeitsrecht
Künstliche Intelligenz, Homeoffice, Arbeit 4.0
Bund Verlag Frankfurt/Main, 8. Aufl. 2022, ISBN 978-3-7663-7272-7, 675 S., 46,00 €

(tw) Inzwischen in der 8. Auflage ist das erstmals 2001 unter dem Titel „Internet und Arbeitsrecht" erschienene Buch von Wolfgang Däubler erhältlich. Dass der Titel sich gewandelt hat und inzwischen das Internet keiner expliziten Erwähnung im Titel bedarf und neue Buzzwords als Untertitel auftauchen ist der rasanten technischen Entwicklung zuzuschreiben, welche die Welt generell, aber eben auch die Arbeitswelt erfasst hat. Das Internet bleibt natürlich präsent, als Kommunikationsbackbone, für die sog. Künstliche Intelligenz (KI), beim Einsatz sozialer Medien, in der Bewerbungssituation, im Homeoffice, beim Robotereinsatz, beim Einsatz privater Geräte im Arbeitskontext (bring your own device), beim Einsatz von virtuellen Realitäten oder beim Crowdworking. Das alles will rechtlich eingehegt sein und es wird tatsächlich auch – oft unvollständig und oft unqualifiziert – geregelt, von Gerichten bewertet und in Betriebsvereinbarungen zwischen Arbeitgebern und Beschäftigten ausgehandelt. Däubler stellt die aktuelle Rechtslage dar, zu der jüngst auch das TTDSG und das Betriebsrätemodernisierungsgesetz gehören.

Wer zu Digitalisierungsfragen im Betrieb Antworten sucht, findet sie in dem Buch. Die Entwicklungen werden thematisiert, die aktuellen Zustände ausführlich beschrieben und erörtert; für die Zukunft wird ein Ausblick gegeben. Das Ganze tut Däubler umfassend und die verschiedenen Seiten beleuchtend. Dabei bleibt aber immer wieder klar, auf welcher Seite er im Streit- oder Konfliktfall steht – auf der Seite der Beschäftigten, wenn es darum geht das rechtliche, finanzielle und organisatorische Übergewicht der Arbeitgeber auszugleichen. Zugleich zeigt Däubler aber auch ein tiefes Verständnis für die Probleme und berechtigten Bedürfnisse der Arbeitgeber, wobei er aus einem großen Schatz eigener Erfahrungen schöpfen kann.

Natürlich ist der Datenschutz ein Schwerpunkt der Darstellung, wobei dieser vom Autor an anderer Stelle, in seinen „Gläsernen Belegschaften" oder in dem von ihm mit herausgegebenen DSGVO/BDSG-Kommentar teilweise detaillierter behandelt wird. Dessen ungeachtet werden alle Datenschutzgrundfragen, die alten wie die sich z.B. mit dem TTDSG neu ergebenden, qualifiziert behandelt. Darüber hinausgehend finden wir in dem Werk Antworten zu weiteren relevanten Fragen: der digitalen Qualifizierung, den Beteiligungsrechten des Betriebs- bzw. Personalrats, dem Schutz in Social Media, der Arbeitszeiterfassung, zum Arbeitsschutz, der unerlaubten Nutzung dienstlicher Geräte, sonstigen möglichen digitalen Pflichtverletzungen des Arbeitnehmers, der Arbeitsvermittlung im Netz und dem Arbeiten als Netzarbeiter oder Fragen der IT-Sicherheit.

Das Ganze wird mit vielen Literatur- und Quellenangaben belegt, so dass weitere Recherchen erleichtert werden. Umfangreiche Verzeichnisse zum Inhalt, zur Literatur und zu Stichworten ermöglichen das schnelle Suchen und qualifizierte Finden. Ein gutes Preis-Leistungsverhältnis macht das Werk nicht nur für Betriebsräte, Arbeitgeber oder IT-ler, sondern auch für einfache Beschäftigte interessant und nützlich.



Klaus, Sebastian/Wittmann, Philipp (Hrsg.)
AufenthV – Aufenthaltsverordnung
Kommentar
C.H.Beck München, 2022
ISBN 978 3 406 77016 6, 530 S., 129,00 €

(tw) Es mag erstaunen, dass in einer Datenschutzzeitschrift ein Kommentar zum Aufenthaltsrecht rezensiert wird. Dies erklärt sich aber leicht mit der Datenschutzrelevanz der Verwaltungsnormen im Ausländerrecht. Zwar liegt der Schwerpunkt des Datenschutzrechts für Ausländerinnen und Ausländer im Ausländerzentral-

registergesetz und in den §§ 86 ff. AufenthG. Insofern liegen brauchbare Kommentierungen vor. Doch diese schon äußerst komplizierten Regelungen sind noch nicht ansatzweise geeignet einen Überblick über die komplexen Informations- und Kommunikationsprozesse zu geben, die bei der Anwendung des Ausländerrechts relevant sind und deshalb für die betroffenen Menschen evtl. existenzielle Bedeutung haben. Viele relevante Normen finden sich in der Aufenthaltsverordnung (AufenthV). Diese ist das „Scharnier" zwischen dem Aufenthaltsgesetz und der Beschäftigungsverordnung, welche die Voraussetzungen bestimmt, nach denen Ausländerinnen und Ausländer in Deutschland zum Arbeitsmarkt zugelassen werden können. Die AufenthV regelt die Passpflichten einschließlich des Umgangs mit Passersatzpapieren für Ausländer und den Angaben, die hierbei aufgenommen und weiterarbeitet werden. Neben weiteren Normen, die nicht für Flüchtlinge, sondern für sonstige Ausländerinnen und Ausländer gelten (z.B. Visumverfahren), bei denen es auch zum personenbezogenen Datenaustausch kommt, sind die Verfahrensvorschriften mit der Kommunikation zwischen den Beteiligten von Relevanz. Die Aufenthaltstitel und alle weiteren Dokumente enthalten Daten, teilweise sensitiver Art wie z.B. Fingerabdrücke oder Lichtbilder, die ausgetauscht und in der Ausländerdateien A und B geführt werden, die unter Behörden ausgetauscht werden und mit denen technische Sicherheitsvorkehrungen einhergehen.

In dem Kommentar von Klaus/Wittmann werden diese Normen aktuell erstmals überhaupt ausführlich dargestellt und kommentiert. Mit kommentiert haben neben den Herausgebern Andreas Dippe, Kim Hammer, Sebastian Röder und Stephanie Tonn. Durch sie kommt ein wenig mehr Licht in den bestehenden Normendschungel bei der Datenverarbeitung und generell der Verwaltung zu Nichtdeutschen. Viele Querverweise zu anderen Normen, etwa im AufenthG, aber auch in europäischen Regelungen oder in weiteren nationalen Spezialgesetzen, erleichtern die Orientierung. Die Sprache ist verständlich, nicht übermäßig juristisch. Es handelt sich nicht um eine kritische, sprich politische Kommentierung, sondern um die kompetente Darlegung des verwaltungsmäßig Vorgesehenen und der administrativen Praxis. Bewertungen erfolgen, werden aber kurz gehalten. Auch die geplanten Änderungen, insbesondere das Aufgehen der Ausländerdatei A in den Ausländerbehörden ins Ausländerzentralregister, werden angesprochen.

Es handelt sich hier um ausgesprochene Speziallektüre. Vorausgesetzt werden einschlägige Spezialkenntnisse, also die Grundlagen des Ausländerrechts wie des Datenschutzrechts. Für Spezialisten ist der Kommentar aber eine wichtige Arbeitshilfe, um Verfahren und insbesondere die Prozesse in der Ausländerverwaltung zu verstehen und einordnen zu können. Damit sollte er zumindest für die ausländerrechtliche Fachanwaltschaft wie für die Migrations-Beratungstätigkeit verfügbar sein.



Schreiber, Kristine/Pommerening, Patrick/Schoel, Philipp
Das neue Recht der Daten-Governance – Data Governance Act (DGA)
Nomos Verlagsgesellschaft, Baden-Baden 2023
ISBN 978-3-8487-8786-9, 162 S., 59,00 €

(ak) Wenn ein Kommentar zu einem neuen Rechtsakt bereits wenige Wochen nach dessen Veröffentlichung erscheint, ist naturgemäß kein umfangreicher Apparat mit Rechtsprechung zu erwarten, schließlich müssen die Urteile erst noch gefällt werden.

Die Autorin und die Autoren des vorliegenden Bandes haben sich auf Basis der genauen Beobachtung des Gesetzgebungsprozesses daran gewagt die neuen Bestimmungen einzuordnen und ihre mögliche Wirkung im Kontext der vorhandenen Rechtsetzung einzuschätzen. Dies ist natürlich umso interessanter, als der DGA selbst nur ein Bestandteil eines größeren Systems ist, von dem wesentliche Teile, insbesondere der Data Act und die Verordnung über den Europäischen Gesundheitsdatenraum, noch im Gesetzgebungsverfahren sind.

Der Kommentar zum DGA ist dennoch hilfreich. Auch wenn noch nicht alle praktischen Fragen der Anwender beantwortet werden können, bietet er einen guten Einstieg in die angestrebte europäische Datenstrategie. Kernfragen des Instruments werden beleuchtet, so die überhaupt nicht einfache Bestimmung des Verhältnisses zwischen dem bestehenden Recht über die Verarbeitung personenbezogener Daten und dem angestrebten Teilen von Daten. Die Frage, wie dieses Verhältnis in praktischen Fällen gestaltet werden kann, und wie Konflikte zwischen beiden Rechtsbereichen gelöst werden können, bedarf in der Tat noch erheblicher Arbeit, die zum Teil auch erst von den Gerichten bewältigt werden kann. Auch das grundsätzlich neue Konzept des Datenaltruismus wird berücksichtigt.

Zielgruppe des Buches sind laut Einführung Unternehmen und Behörden, die von den Bestimmungen des DGA betroffen sind. Der Band mag aber auch den an den anderen Gesetzgebungsverfahren Beteiligten helfen die Bestimmungen des DGA schnell nachzuschlagen.

In einer Folgeauflage soll der Data Act berücksichtigt werden, ohne den der DGA seine Wirkung kaum entfalten kann. Der vorhandene Kommentar kann zur Vorbereitung auf die Auseinandersetzung mit der komplexeren Datenstrategie dienen.

Insgesamt ist der Kommentar gut lesbar, und dank eines umfangreichen Index auch als Nachschlagewerk geeignet.

Welche Maßnahmen ergreift ChatGPT zum Datenschutz?

Antwort von ChatGPT:
„Als KI-Sprachmodell, das von OpenAI entwickelt wurde, nimmt ChatGPT den Datenschutz sehr ernst. OpenAI hat umfassende Maßnahmen ergriffen, um sicherzustellen, dass die von ChatGPT verarbeiteten Daten geschützt sind.
Zunächst wird ChatGPT von einem Team von Sicherheitsexperten überwacht, die kontinuierlich die Systeme und Prozesse von OpenAI auf Schwachstellen und Bedrohungen überwachen. OpenAI verwendet auch branchenübliche Sicherheitsprotokolle wie Firewalls, Verschlüsselung und Zugriffskontrollen, um sicherzustellen, dass die von ChatGPT verarbeiteten Daten sicher sind.
Darüber hinaus nimmt OpenAI den Datenschutz sehr ernst und hat umfassende Datenschutzrichtlinien und -verfahren implementiert, um sicherzustellen, dass die Daten, die von ChatGPT verarbeitet werden, geschützt und vertraulich bleiben. OpenAI bietet Benutzern auch die Möglichkeit, ihre Daten zu löschen, und gibt ihnen Kontrolle darüber, wie ihre Daten verwendet werden.
Zusammenfassend lässt sich sagen, dass OpenAI und ChatGPT umfangreiche Maßnahmen ergreifen, um die Sicherheit und den Datenschutz der von ChatGPT verarbeiteten Daten zu gewährleisten.“

Das Bild auf dieser Seite wurde von der OpenAI-Anwendung DALL-E nach den Vorgaben „Hund mit Brille und Hut“ automatisiert generiert. Hierbei zeigt sich, dass künstliche Intelligenz nicht nur eine Herausforderung für den Datenschutz sondern auch für das Urheberrecht ist.

